公安院校
招录培养体制改革
试点专业
系列教材

计算机犯罪侦查方向

丛书主编 李锦

信息网络安全管理

黄波 主编 / 刘洋洋 纪芳 副主编

清华大学出版社

公安院校招录培养体制改革试点专业系列教材

信息网络安全管理

黄　波　主　编
刘洋洋　纪　芳　副主编

清华大学出版社
北　京

内 容 简 介

本书系统地介绍了信息网络安全管理工作中涉及的业务内容、流程标准和规范，主要包括信息网络安全概念，信息网络安全保障体系构成，信息网络安全管理措施，信息网络安全法律法规体系，网络安全监督管理的内容、任务和方法，互联网信息内容安全体系及互联网有害信息和热点信息的查处与管理，互联网上网营业服务场所安全监管，信息安全等级保护工作，信息网络安全违法案件查处等涉及网络安全管理与执法中的知识。全书内容翔实，涵盖面广。

本书可以作为公安院校招录培养体制改革网络犯罪侦查专业学生的教材，也可以作为公安院校、普通高校相关专业本、专科学生的教材和教学参考书及公安民警普及信息网络安全管理知识、了解信息网络安全保卫工作的参考书。

图书在版编目(CIP)数据

信息网络安全管理/黄波主编. —北京：清华大学出版社，2013.2
(公安院校招录培养体制改革试点专业系列教材)
ISBN 978-7-302-29345-3

Ⅰ. ①信… Ⅱ. ①黄… Ⅲ. ①信息网络－安全管理－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2012)第 157008 号

责任编辑：闫红梅 李 晔
封面设计：
责任校对：梁 毅
责任印制：

出版发行：清华大学出版社
网 址：http://www.tup.com.cn，http://www.wqbook.com
地 址：北京清华大学学研大厦 A 座 **邮 编：**100084
社 总 机：010-62770175 **邮 购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：
装 订 者：
经 销：全国新华书店
开 本：185mm×230mm **印 张：**12.25 **字 数：**270 千字
版 次：2013 年 2 月第 1 版 **印 次：**2013 年 2 月第1 次印刷
印 数：1～ 000
定 价： .00 元

产品编号：043369-01



期待已久的由李锦同志主编的《公安院校招录培养体制改革试点专业系列教材》终于出版了！该系列教材是我国第一套计算机犯罪侦查专业系列教材，它的出版解决了国内相关院校教师与学生急需的教课书问题，也为从事信息安全专业和侦查执法人员提供一套极有价值的参考丛书。这实属一件可喜可贺的事！

由于信息技术空前迅速的发展，极具挑战的计算机网络空间形成了一个变幻无穷的虚拟空间。现实社会中的犯罪越来越多地涉及到计算机、手机等工具，各种数字技术与网络虚拟空间的交汇，使计算机犯罪侦查技术变得空前重要与紧迫。从20世纪90年代兴起的数字取证调查，涌现出各种各样的技术和工具，使得数字取证成为计算机专业的一门新兴学科。国际上的一些大学近年来已设置了专门的系和研究生学位的授予，为计算机犯罪侦查的教学内容增添了丰富而又精彩的情景。他山之石可以攻玉，许多技术和教材可以借鉴，但数字取证牵涉到法学、法规，各国的国情不尽相同，唯一的解决办法就是必须自主创新、撰写适合国内需要的相应教材。

面临这一劈山开路的挑战，本教材从专业的技术层面为国内的本科生尝试提供全面的教学培训，内容包括了从互联网体系结构原理到电子商务应用与各种法规，以及计算机网络攻防技术与信息系统安全等级保护与管理等基础知识，重点围绕着计算机犯罪调查的手段、工具与方法以及数据证据的分析与鉴定等基础知识；教材注重在传授理论知识的同时，强化面向实战能力的培训，全套教材既适应了学科特点又考虑到学生层次的具体情况，处处反映出作者们的精心思索。

本系列教材参编的作者全部来自辽宁警官高等专科学校的师资队伍，该校地处辽东半岛，面临蓝色的大海，大浪淘沙涌现一批时代的人杰。庄严整洁的校园具有公安教育突出的特色，更为可贵的是他们倡导教学、科研、警务实践紧密结合，不断创新教学模式的一贯校风，每年从那里培养出大量信息时代专业特色明显、创新能力强的人才队伍。本套系列教材的出版充分体现了该校的学术水平与精神面貌，尤其映射出参编作者们拥有第一线资深的教学经验和扎实的实际专业知识，以及始终保持一股奋发上进、开拓创新的风范。我在此由衷地对本教材的出版表示祝贺，并预祝他们再接再厉，取得更加辉煌的成功！

许榕生

2012-6 写于北京

前言



随着计算机和网络通信技术的快速发展，信息网络在社会政治、经济、文化以及生活中发挥着愈来愈重要的作用，信息网络的发展极大地提高了我国的综合国力。同时因信息网络的开放性、互连性，进入21世纪后我国国内政治、经济、军事、科技等重要领域网络安全保护能力不强、信息网络安全技术的落后、信息网络安全保障政策及法律建设不协调、个人信息网络安全意识淡化等因素给国家安全和社会稳定带来了威胁。如何实现信息网络的安全有效运行成为当前保障国家安全和社会稳定发展的主要问题。

目前我国信息网络安全面临着严峻的挑战。特别是近年来，我国网络犯罪不断呈上升趋势，各种传统犯罪与网络犯罪结合的趋势日益明显，网络诈骗、网络盗窃等侵害他人财产的犯罪增长迅速，制作传播计算机病毒、入侵和攻击计算机与网络的犯罪日趋增多，利用互联网传播淫秽色情及从事赌博等犯罪活动仍然突出。据统计，1998年公安机关办理各类网络犯罪案件142起，2007年增长到2.9万起，2008年为3.5万起，2009年为4.8万起。

信息网络安全管理是国家法律法规赋予公安机关的一项重要职能，是公安机关在信息网络领域承担的一项重要的工作。公安机关要依照信息安全法律法规对互联网运营单位、联网服务单位、联网单位，上网营业服务场所和重要的信息系统依法进行管理，依法打击网络违法犯罪行为，在虚拟空间建立“打防结合”的安全保障机制，为我国信息网络健康发展保驾护航。

本书是编者在多年教学、研究积累的基础上，紧密围绕公安工作，结合在公安一线实习和挂职锻炼的学习心得，深刻体会信息网络安全保障体系的建设与应用的思路，紧密围绕信息网络安全管理这一公安工作的流程和业务需要，围绕实践编写的一本具有理论和实践指导意义的教程。

本书共包括7章内容，其中，第1章由黄波、杨虹编写；第2章和第6章由黄波、卢睿编写；第4章和第7章由刘洋洋编写；第3章和第5章由纪芳编写；全书由黄波统稿。在编写过程中得到了米佳教授的支持与帮助，在此表示衷心感谢。

由于编写水平和时间有限，书中难免有疏漏和不妥之处，敬请广大读者提出宝贵意见。

编者

2012年3月



第 1 章　信息网络安全管理概述 ········ 1

1.1　信息网络安全问题 ········ 1
1.1.1　信息网络安全现状 ········ 1
1.1.2　信息网络安全的概念 ········ 2
1.1.3　信息网络安全的层次 ········ 4
1.1.4　信息网络安全的特征 ········ 5
1.2　信息网络面临的不安全因素 ········ 6
1.2.1　信息网络自身的脆弱性 ········ 6
1.2.2　信息网络系统面临的威胁 ········ 7
1.3　信息网络安全保障体系结构 ········ 8
1.3.1　OSI 网络保障体系结构 ········ 8
1.3.2　P2DR 模型 ········ 12
1.3.3　WPDRRC 模型 ········ 13
1.4　信息网络安全的策略 ········ 14
1.4.1　信息网络安全管理 ········ 15
1.4.2　信息网络安全技术 ········ 18
习题 ········ 21

第 2 章　信息网络安全法律法规 ········ 22

2.1　信息网络安全法律法规体系 ········ 22
2.1.1　信息网络安全法律法规概述 ········ 22
2.1.2　我国信息网络安全法律法规 ········ 23
2.2　信息网络安全法律法规与部门规范 ········ 24
2.2.1　信息网络安全相关国家法律 ········ 24
2.2.2　信息网络安全相关行政法规 ········ 26
2.2.3　信息网络安全相关部门规范与其他规范 ········ 28

习题 …………………………………………………………… 31

第 3 章　网络安全监督管理 …………………………………… 32

3.1　网络安全监督管理概述…………………………………… 32
3.1.1　网络安全监督管理指导思想 ………………………… 32
3.1.2　网络安全监督管理工作特点 ………………………… 33
3.1.3　网络安全监督管理主要任务 ………………………… 34
3.1.4　网络安全监督管理主要方法 ………………………… 34
3.2　互联网单位管理…………………………………………… 36
3.2.1　备案管理 ……………………………………………… 36
3.2.2　互联网运营单位管理 ………………………………… 46
3.2.3　互联网信息服务单位管理 …………………………… 56
3.2.4　联网单位管理 ………………………………………… 66
3.3　计算机病毒等破坏性程序防治管理……………………… 71
3.3.1　管理依据 ……………………………………………… 71
3.3.2　管理对象 ……………………………………………… 71
3.3.3　管理职责 ……………………………………………… 71
3.3.4　工作要求 ……………………………………………… 72
3.3.5　行政处罚 ……………………………………………… 73
3.4　计算机安全员培训及管理………………………………… 75
3.4.1　培训目的 ……………………………………………… 75
3.4.2　培训对象 ……………………………………………… 75
3.4.3　培训内容 ……………………………………………… 75
3.4.4　培训方式及要求 ……………………………………… 76
3.4.5　计算机安全员的管理 ………………………………… 76
习题 …………………………………………………………… 77

第 4 章　互联网信息内容安全管理 …………………………… 78

4.1　互联网信息内容安全管理概述…………………………… 78
4.1.1　互联网信息内容安全管理基本概念 ………………… 78
4.1.2　国外互联网信息内容安全管理现状 ………………… 79
4.1.3　我国互联网信息内容安全管理基本原则 …………… 83
4.2　互联网信息内容安全管理体系…………………………… 84
4.2.1　互联网信息内容安全管理机构及职责 ……………… 84
4.2.2　互联网信息内容安全管理法律框架 ………………… 86

4.2.3　互联网信息服务单位安全管理制度 ………………………………… 88
4.3　互联网有害信息查处…………………………………………………… 94
4.3.1　互联网有害信息的概念和特征 …………………………………… 94
4.3.2　互联网有害信息的界定 …………………………………………… 95
4.3.3　互联网有害信息处置 ……………………………………………… 97
4.3.4　互联网有害信息举报投诉及案件报告与协助查处制度 ………… 98
4.4　互联网热点信息管理…………………………………………………… 98
4.4.1　互联网热点信息的概念和特征 …………………………………… 98
4.4.2　互联网热点信息的搜集与编报 …………………………………… 99
习题……………………………………………………………………………… 102

第 5 章　互联网上网服务营业场所安全管理………………………………… 103

5.1　概述 ……………………………………………………………………… 103
5.1.1　互联网上网服务营业场所及发展概况……………………………… 103
5.1.2　互联网上网服务营业场所的安全问题……………………………… 105
5.2　互联网上网服务营业场所安全管理 …………………………………… 108
5.2.1　管理依据………………………………………………………………… 108
5.2.2　管理职能………………………………………………………………… 110
5.2.3　互联网上网服务营业场所信息网络安全管理……………………… 113
5.2.4　互联网上网服务营业场所治安安全管理…………………………… 116
5.2.5　互联网上网服务营业场所消防安全管理…………………………… 117
5.3　互联网上网服务营业场所安全监管 …………………………………… 119
5.3.1　安全审核………………………………………………………………… 119
5.3.2　日常监管………………………………………………………………… 122
5.3.3　基础资料管理…………………………………………………………… 134
5.4　违反互联网上网服务营业场所安全管理的处罚 ……………………… 134
5.4.1　刑事处罚………………………………………………………………… 134
5.4.2　行政处罚………………………………………………………………… 134
5.4.3　法律责任………………………………………………………………… 135
习题……………………………………………………………………………… 136

第 6 章　信息安全等级保护管理……………………………………………… 137

6.1　信息安全等级保护制度 ………………………………………………… 137
6.2　信息安全等级保护政策与标准 ………………………………………… 140
6.2.1　信息安全等级保护政策体系………………………………………… 140

6.2.2　信息安全等级保护标准体系 …… 142
6.3　信息系统等级保护工作 …… 146
6.3.1　信息系统等级保护工作的要求与职责 …… 146
6.3.2　信息系统等级保护工作流程 …… 149
习题 …… 164

第7章　信息网络安全违法犯罪案件查处 …… 165

7.1　案件查处工作概述 …… 165
7.1.1　信息网络案件的概念 …… 165
7.1.2　信息网络案件管理依据 …… 165
7.1.3　信息网络案件管辖范围 …… 165
7.1.4　信息网络案件分类 …… 166
7.2　主要信息网络犯罪案件及其处罚标准 …… 166
7.2.1　以计算机信息网络系统为对象的案件 …… 166
7.2.2　以计算机信息网络系统为工具的案件 …… 168
7.3　主要信息网络违法案件及其处罚标准 …… 179
7.3.1　利用信息网络扰乱公共秩序的案件 …… 179
7.3.2　利用信息网络侵犯人身权利、财产权利的案件 …… 180
7.3.3　利用信息网络妨害社会管理的案件 …… 180
习题 …… 182

参考文献 …… 183

第 1 章

信息网络安全管理概述

【内容提要】

本章介绍了信息网络安全的发展现状、保障体系、安全措施。通过学习，要求学生了解信息网络安全的概念及层次划分，掌握信息网络安全保障体系结构及措施。

1.1 信息网络安全问题

信息网络安全目前已成为信息时代人类共同面临的新挑战。信息网络在我国政治、经济、文化以及社会生活中发挥着愈来愈重要的作用，作为国家关键基础设施和新的生产、生活工具，信息网络的发展极大地促进了信息传递和共享，提高了社会生产效率和人民生活水平，促进了经济社会的发展。信息网络的影响日益扩大、地位日益提升，维护信息网络安全工作的重要性日益突出，同时信息网络中的不安全因素也使得世界各行各业的安全受到严重威胁，如何实现信息网络的安全有效运行成为当前保障国家安全和社会稳定发展的主要问题。

1.1.1 信息网络安全现状

随着科学技术的发展，信息网络技术进入了高速发展的时期。信息网络是人类智慧的结晶，20 世纪的重大科技发明，当代先进生产力的重要标志。人们对信息网络安全的需求从单一的通信保密，发展到今天的信息网络安全产品、技术手段等多方面。

在信息网络飞速发展的同时，信息网络安全也引起了人们的普遍关注。据有关方面统计，美国每年因网络安全问题而遭受的经济损失超过 170 亿美元，德国、英国也均在数十亿美元以上，法国大约为 100 亿法郎，日本、新加坡等国的问题也很严重。在国际刑法界列举的现代社会新型犯罪排行榜上，计算机犯罪已名列榜首。据统计，全球平均每 20 秒就发生 1 次网上入侵事件，黑客一旦找到系统的薄弱环节，所有用户均会遭殃。

互联网在我国得到了飞速发展：到 2012 年 6 月底中国网民人数达到 5.38 亿，中国手机网民规模达到 3.88 亿，国际出口带宽达到 1 548 811Mbps，中国网站规模达到 250.3 万个，“.CN”域名注册量达到 398 万个。我国网络安全同样也面临着巨大的威胁。据不完全统计，2009 年中国被境外控制的计算机 IP 地址达 100 多万个；被黑客篡改的网站达 4.2 万

个；被“飞客”蠕虫网络病毒感染的计算机每月达 1800 万台，约占全球感染主机数量的 30%。公安机关办理的各类网络犯罪案件也呈上升趋势：1998 年 142 起，2007 年增长到 2.9 万起，2008 年为 3.5 万起，2009 年为 4.8 万起。2010 年，我国互联网上出现病毒 750 万个，受害网民 7.03 亿人次，被挂马网站 3382 万个，钓鱼网站 175 万个。病毒与经济利益深度结合，商业公司成为黑客套现的主要手段。

2009 年 1 月，中国政府开始发放第三代移动通信(3G)牌照，目前 3G 网络已基本覆盖全国。网民上网方式已从最初以拨号上网为主，发展到以宽带和手机上网为主。移动设备的快速普及，使得移动互联网与互联网之间的界限越来越模糊，而肆虐互联网的木马和网络钓鱼开始侵入移动互联网领域，截至 2010 年 11 月，新增手机病毒 1513 个，累积病毒数量达 2357 个，累计感染手机 800 万部以上。

因此，采取各种措施加强信息网络安全已是当务之急。

1.1.2 信息网络安全的概念

信息网络安全涉及到国家、社会、企业和个人生活等各个领域，从本质上说就是保护信息网络系统中硬件、软件和系统中数据的安全。从广义的角度，凡是涉及信息网络的保密性、完整性、可用性、可控性、不可否认性的相关技术和理论都是信息网络安全所要研究的领域，这五个特性也是信息网络安全所要达到的目标。从国家和社会的角度，信息网络安全就是要保护国家和社会的信息安全，避免威胁国家安全、社会稳定；从企业团体的角度，保护企业的商业机密、经济利益和企业的品牌声誉，避免出现病毒、非法读写、拒绝服务、资源非法占用及非法控制等现象；从个人的角度，就是要保护个人隐私和利益，避免他人利用窃听、冒充、篡改等手段损害个人利益。

因此，信息网络安全在不同的环境和应用中有不同的含义，《中华人民共和国计算机信息系统安全保护条例》的第三条规范了包括计算机网络系统在内的计算机信息系统安全的概念：“计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施(含网络)的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。”

信息网络安全具有以下五个特性，这也是信息网络安全所要达到的目标。

保密性(Confidentiality)：指保证关键信息和敏感信息不被非授权者获取、解析或恶意利用。

完整性(Integrity)：指保证信息从真实的信源发往真实的信宿，在传输、存储过程中未被非法修改、替换、删除；信息完整性是信息网络安全的基本要求。破坏信息的完整性是影响信息网络安全的常用手段。

可用性(Availability)：指保证信息和信息系统随时可为授权者提供服务而不被非授权者滥用和阻断。

可控性(Access Control)：即对信息、信息处理过程及信息系统本身都可以实施合法的安全监控和检测。

不可否认性(Non-repudiation)：保证出现信息网络安全问题后可以有据可查，可以追踪责任到人或到事，又称信息的抗抵赖性。

具体来说，信息网络安全保护的对象是信息。其中信息的保密性、完整性和可用性是保证信息网络安全的基本特性。此外还包括可控性、合法性、不可否认性等特性。

信息的保密性针对信息被允许访问对象的多少而不同。所有人员都可以访问的信息为公开信息，需要限制访问的信息一般为敏感信息或秘密。秘密可以根据信息的重要性及保密要求分为不同的密级，例如，国家根据秘密泄露后对国家经济、安全利益产生的影响及后果不同，将国家秘密分为秘密、机密和绝密三个等级，组织可根据其信息网络安全的实际，在符合《国家保密法》的前提下将其信息划分为不同的密级；对于具体信息的保密性有时效性，如秘密到期即可解密等。

信息的完整性主要包括两方面：一方面是指信息在利用、传输、存储等过程中不被篡改、丢失或缺损等；另一方面是指信息处理的方法的正确性，不正当的操作，如误删除文件，有可能造成重要文件的丢失。

信息的可用性指信息及相关的信息资产在授权人需要时，可以立即被获得。例如，通信线路中断故障会造成信息在一段时间内不可用，影响正常的商业运作，这是信息可用性的破坏。

信息的可控性主要指对危害国家的信息进行监视审计，控制授权范围内信息的流向及行为方式，使用授权机制，控制信息传播的范围、内容。

信息的不可否认性是对出现的安全问题提供调查的依据和手段，使用审计、监控、防抵赖等安全机制，使得攻击者、破坏者无法抵赖，从而实现信息网络安全的可审计性。

信息的合法性是保证信息内容和制作、发布、复制、传播信息的行为符合宪法和法律的规定。我国的信息网络安全具有中国特色，不仅包括信息、数据安全的本身属性，还具有社会对信息网络安全所要求的“内容合法性”。我国现有信息网络安全法律规范对信息的合法性有明确规定，任何人不得利用信息网络制作、发布、复制、传播违反宪法和法律规定的信息。信息发送应事先取得信息接收者的授权。任何单位和个人不得利用电子邮件、通信短信息等信息服务方式发送未经信息接收者事先授权或者不能有效拒绝的信息。

信息网络安全的侧重点和重视程度会随着使用者的需求而变。如某些专有技术、市场营销计划等商业秘密，其保密性尤其重要；对于工业自动控制系统，控制信息的完整性相对其保密性重要得多；而对于瞬息万变的金融证券市场来说，保证信息的可用性是用户的第一需求；对网络运行和管理者来说，在使用过程中希望本地网络信息的访问、读、写等操作受到保护和控制；电子商务交易过程中的一些协议和合同的签署过程中不可否认性尤为重要；电子出版过程中的著作权使用的合法性非常关键。

1.1.3　信息网络安全的层次

为了使信息网络实现上面提到的五大特性,必须从物理设备、网络、系统、应用和管理各层面出发,保证各层面的安全。信息网络安全层次如图 1-1 所示。

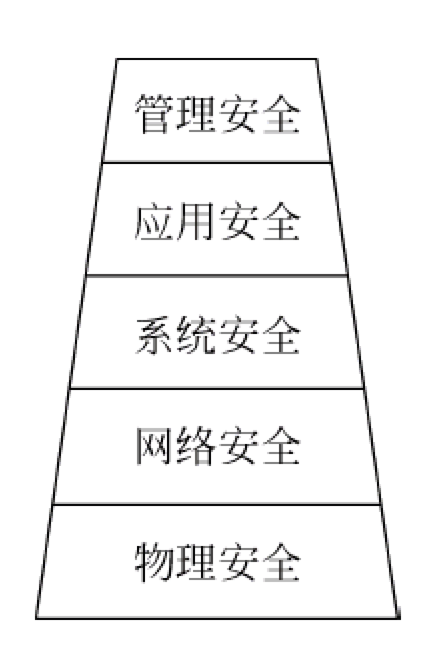


图 1-1　信息网络安全层次

1. 物理安全

物理安全是保护计算机设备、设施(含网络)以及其他媒体等实体免遭地震、水灾、火灾等环境事故(如电磁污染等),以及因为操作失误或各种计算机犯罪行为导致破坏的措施和过程。为了保证实体安全必须做到环境安全、设备安全和媒体安全,其用来保证硬件和软件本身的安全,是整个信息网络安全的基石。

2. 网络安全

网络安全的组成如图 1-2 所示。

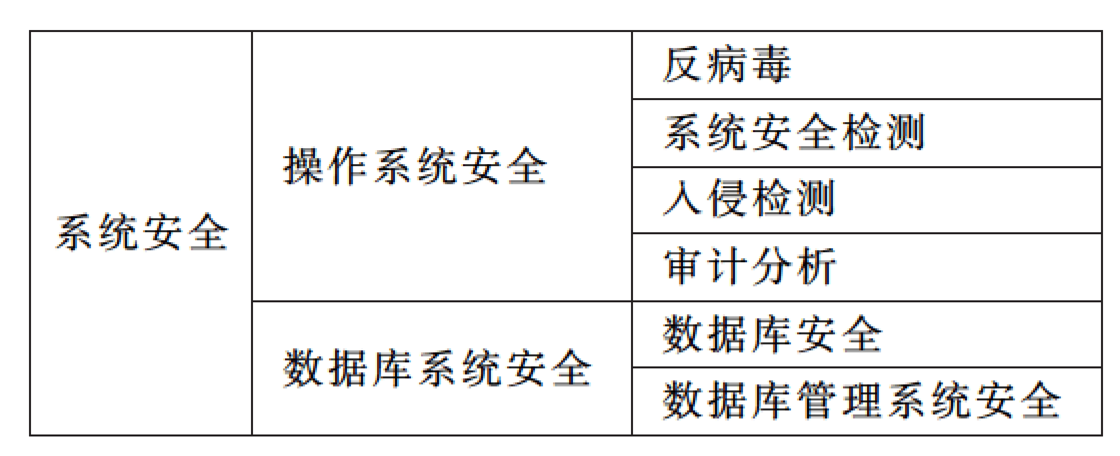
网络安全	局域网、子网安全	访问控制安全
		网络安全检测
	网络中数据传输安全	数据加密
	网络运行安全	备份与恢复
		应急
	网络协议安全	TCP/IP
		其他协议

图 1-2　网络安全的组成

在网络安全中,在内网和外网之间,设置合理的访问控制,可使内网对外网和外网对内网的访问都变得安全可靠又具有实用性。网络安全检测通常对内网的硬件和软件进行安全评估,检测出存在的漏洞和潜在的威胁,以达到增强网络安全的目的。数据备份不仅在网络系统硬件故障或因为失误时起到保护作用,也在入侵者实施非授权访问或对网络进行攻击及破坏数据完整性时起到保护作用,使网络系统及时获得恢复。互联网采用的主流协议是TCP/IP,其设计初期强调开放性和便利性,没考虑安全性,因此协议存在严重安全漏洞,给网络安全留下隐患。

3. 系统安全

系统安全的组成如图 1-3 所示。



系统安全	操作系统安全	反病毒
		系统安全检测
		入侵检测
		审计分析
	数据库系统安全	数据库安全
		数据库管理系统安全

图 1-3　系统安全的组成

用户常用的系统包括操作系统和数据库系统两种。

一般用户对操作系统的安全还比较重视，但对数据库系统的安全并不重视，实际上，数据库系统作为许多应用系统的底层平台其安全性也十分重要。

4. 应用安全

应用安全的组成如图 1-4 所示。

应用安全	应用软件开发平台安全	各种编程语言平台安全
		程序本身的安全
	应用系统安全	应用软件系统安全

图 1-4　应用安全的组成

应用安全建立在系统平台之上，人们普遍会重视系统安全，而忽视应用安全。主要原因包括两个方面：第一，对应用安全缺乏认识；第二，应用系统过于灵活，需要较高的安全技术。恰恰因为应用程序存在很多漏洞，其配置也会存在很多问题，通常容易成为恶意软件攻击或利用的目标。只有通过及时的更新才能避免受到攻击。

5. 管理安全

管理安全是信息网络安全体系中不可缺少的一部分。完整的信息网络安全解决方案不仅包括物理安全、网络安全、系统安全和应用安全等这些技术手段，还需要以人为核心的策略和管理支持。网络安全至关重要的往往不是技术手段，而是对人的管理。

1.1.4　信息网络安全的特征

综合来看，信息网络安全具有以下特征：

(1) 信息网络安全是多维的安全。

信息网络安全是一个系统问题。一个安全的信息系统不仅仅要考虑环境安全和技术安全，还要考虑管理安全的问题；一个安全的信息系统不仅仅能够提供静态的保护能力，还需要具备主动防御的能力，能够及时发现攻击，并能够从破坏中恢复。

(2) 信息网络安全是动态的安全。

从信息系统的角度看,信息网络安全不是一个静止的状态,它是一个动态变化的过程。从历史的角度看,信息网络安全也不是一个静止的概念,它随着信息技术的进步而发展,随着产业基础、用户认识、投入产出的不同而变化。

(3) 信息网络安全是相对的安全。

信息网络安全是相对的,由于技术局限性、环境复杂性以及需求变化等因素的限制,目前现实世界中不存在百分之百的绝对安全。信息网络安全通常是指一定程度上的安全,如遵循适度安全原则的信息网络安全强调的是适度安全,实现投入产出平衡。

(4) 信息网络安全是过程的安全。

信息网络安全不是一个孤立的问题,应在系统建设过程中加以同步考虑,从规划设计阶段开始一直到系统终止,贯穿整个信息系统的生命周期。

(5) 信息网络安全是无国界的安全。

信息网络安全是无国界的。Internet 在发挥重大积极作用的同时,消极作用也体现了世界性和国际性,如网上攻击事件大幅上升。信息网络安全不是一个国家能完全控制的问题,具有全球化特点,应从全球信息化角度考虑和布局。

(6) 信息网络安全是多层次的安全。

与只涵盖保密性的狭义信息网络安全不同,广义的信息网络安全是一个宽泛的概念。不同层次的主体从不同角度分析不同的对象,会导致对信息网络安全有着不同的理解。如从主体层次看,国家层面的信息网络安全是指维护国家基础设施相关信息系统的安全,保障国家不受信息战争的威胁;国家机关、企事业单位层面的信息网络安全关注的是其负责建设和维护的信息系统的安全,确保信息的保密性以及服务的及时性与有效性;而个人层面的信息网络安全主要是指保护个人隐私。一般情况下,信息网络安全是指某个特定环境中的指定信息系统的安全。

1.2 信息网络面临的不安全因素

导致信息网络安全问题的主要因素是信息网络自身的脆弱性和信息网络面临的威胁。

1.2.1 信息网络自身的脆弱性

信息网络自身的脆弱性主要指网络系统和设备、计算机软硬件在设计时由于考虑不周等留下的缺陷,容易被威胁主体所利用从而危害系统的正常运行。其主要包括以下几个方面:

1. 计算机硬件系统及网络物理环境的脆弱性

计算机硬件本身存在易丢失、易损坏,且本身没有为对其访问和使用设计防护措施,以

及硬件漏磁等缺陷；网络物理环境也存在脆弱性，包括温度、湿度、灰尘、静电、电磁干扰、雷电、火灾、水患等对网络硬件设备和信息网络安全的影响。

2. 计算机网络和信息传输中的脆弱性

TCP/IP 协议本身的开放性带来的脆弱性。主要体现在信息输入、处理、传输、存储、输出过程中存在的信息容易被篡改、伪造、破坏、窃取、泄漏等不安全因素，包括信息泄漏、电子干扰等。

3. 计算机操作系统和软件系统的脆弱性

包括信息系统自身运行所需要的操作系统、数据库管理系统以及系统应用软件自身存在的漏洞及使用不当等造成的不安全因素。

4. 信息网络安全管理的脆弱性

由于信息网络使用人员繁杂、网络安全技术素质及安全意识参差不齐，导致信息网络安全管理的脆弱性。

另外，网络安全的脆弱性还和网络的规模有密切关系，网络规模越大，其脆弱性越大。

1.2.2　信息网络系统面临的威胁

目前信息网络面临的威胁主要包括来自电磁泄露、雷击等环境因素构成的威胁，软硬件故障和工作人员误操作等人为或偶然事故构成的威胁，利用计算机实施盗窃、诈骗等违法犯罪活动的威胁，网络攻击和计算机恶意代码构成的威胁以及信息战的威胁等，概括起来主要有以下几类。

1. 内部泄密和破坏

包括内部涉密人员有意或无意泄密、更改记录信息；内部非授权人员有意偷窃机密信息、更改记录信息；内部人员破坏信息系统等。

2. 截获

网络攻击者可能通过搭线或在电磁波辐射范围内安装截收装置等方式，截获机密信息，或通过对信息流量和流向、通信频度和长度等参数的分析，推出有用信息。

3. 非法访问

未经授权使用信息资源或以未授权的方式使用信息资源，它包括非法用户（通常称为黑客）进入网络或系统进行违法操作、合法用户以未授权的方式进行操作。

4. 破坏信息的完整性

网络攻击者通过篡改、删除、插入等操作破坏信息的完整性。

5. 冒充

冒充领导发布命令、调阅密件，冒充主机欺骗合法主机及合法用户，冒充网络控制程序套取或修改使用权限、口令、密钥等信息，越权使用网络设备和资源等。

6. 破坏系统的可用性

网络攻击者破坏网络系统的可用性，使合法用户不能正常访问网络资源，使有严格时间

要求的服务不能及时得到响应等。

7. 其他威胁

对信息网络系统的威胁还包括计算机病毒、电磁泄漏、各种灾害、操作失误等。

1.3 信息网络安全保障体系结构

为了保证信息网络安全策略得以完整准确地实现,安全需求得以全面准确地满足,人们开始对信息网络安全体系进行研究,希望通过对信息网络安全体系的功能、服务、安全机制、技术、管理和操作,以及这些因素在整个体系中的合理部署和相互关系的研究,为信息安全的解决方案和工程实施提供依据和参考。

1.3.1 OSI 网络保障体系结构

国际标准化组织(ISO)制定了开放系统互连(OSI)参考模型,将计算机网络分为七个层次以实现网络互联。1989 年该组织提出了 OSI 安全体系结构:ISO 7498—2:1989。该标准被我国等同采用,即《信息处理系统—开放系统互连—基本参考模型—第二部分:安全体系结构 GB/T 9387.2—1995》。作为 OSI 参考模型的新补充,ISO 7498—2 标准现在已经成为网络安全专业人员的重要参考,它不是解决某一特定的安全问题,而是为解决网络安全共同体提出了一组公共的概念和术语,用来描述和讨论安全问题和解决方案。OSI 安全体系结构主要包括三部分内容,即安全服务、安全机制和安全管理,三者关系如图 1-5 所示。

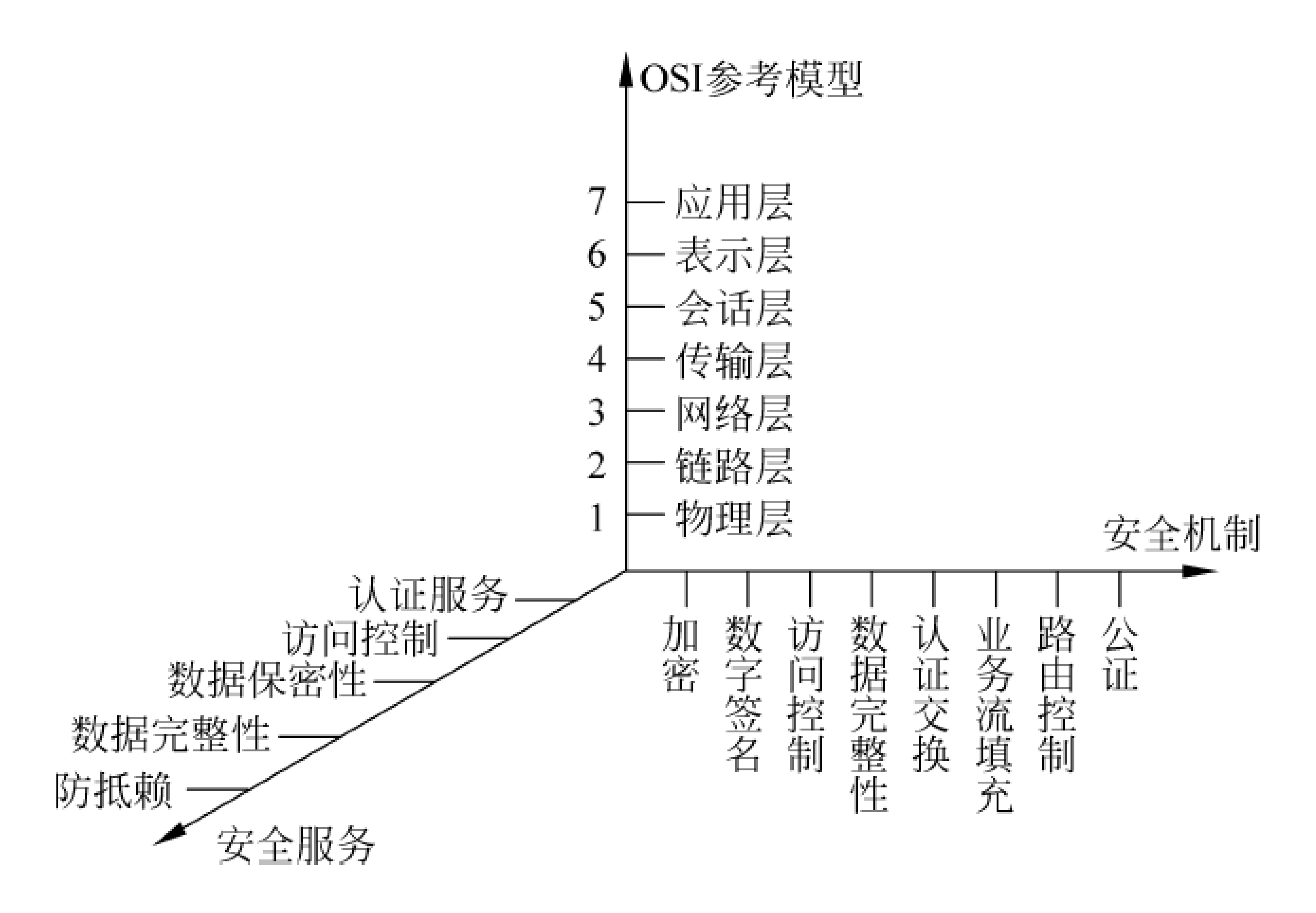


图 1-5 OSI 安全体系结构

1. 安全服务

ISO 对 OSI 规定了五种级别的安全服务,安全服务与 OSI 七层的关系如表 1-1 所示。

表 1-1　OSI 安全体系结构中安全服务与层次

安全服务		OSI 层次						
		1	2	3	4	5	6	7
认证服务	对等实体认证			√	√		√	
	数据源认证			√	√			√
访问控制	访问控制服务			√	√		√	√
数据保密性	连接保密	√	√	√	√		√	
	无连接保密		√	√	√		√	
	选择字段保密							√
	业务流保密	√		√				√
数据完整性	可恢复连接完整性				√			
	无恢复连接完整性			√	√		√	
	选择字段连接完整性						√	
	无连接完整性			√	√		√	
	选择字段无连接完整性						√	
防抵赖	源发方的抗抵赖							√
	接收方的抗抵赖							√

1）认证安全服务

认证安全服务是防止主动攻击的重要措施，这种安全服务提供对通信中的对等实体和数据来源的鉴别，它对于开放系统环境中的各种信息安全有重要的作用。认证就是识别和证实。识别是辨别一个对象的身份，证实是证明该对象的身份就是其声明的身份。OSI 环境可提供对等实体认证和信源认证的安全服务。

2）访问控制安全服务

访问控制安全服务是针对越权使用资源和非法访问的防御措施。访问控制大体可分为自主访问控制和强制访问控制两类。其实现机制可以是基于访问控制属性的访问控制表或基于安全标签、用户分类和资源分档的多级访问控制等。访问控制安全服务主要位于应用层、传输层和网络层。它可以放在通信源、通信目标或两者之间的某一部分。

3）数据保密性安全服务

数据保密性安全服务是针对信息泄露和窃听等被动威胁的防御措施。这组安全服务又细分为：

（1）信息保密——保护通信系统中的信息或网络数据库数据。而对于通信系统中的信息，又分为面向连接保密和无连接保密。连接保密服务为一次连接上的全部用户数据保证其机密性。

（2）数据选择字段保密——保护信息中被选择的部分数据字段；这些字段或处于连接的用户数据中或为单个无连接的 SDU（一体化采集器）中的字段。

(3) 业务流保密——防止攻击者通过观察业务流，如信源、信宿、转送时间、频率和路由等来得到敏感的信息。

4) 数据完整性安全服务

数据完整性安全服务是针对非法地篡改和破坏信息、文件和业务流而设置的防范措施，以保证资源的可获得性。这组安全服务又细分为：

- 可恢复面向连接的完整性。
- 无恢复面向连接的完整性。
- 选择字段面向连接的完整性。
- 无连接完整性。
- 选择字段无连接完整性。

5) 防抵赖安全服务

防抵赖安全服务是针对对方进行抵赖的防范措施，可用来证实已发生过的操作。这组安全服务可细分为：

(1) 源发方的防抵赖，它为数据的接收者提供数据来源的证据，这将使发送者谎称未发送过这些数据或否认它的内容的企图不能得逞。

(2) 接收方的防抵赖，它为数据的发送者提供数据交付证据，这将使得接收者事后谎称未收到过这些数据或否认内容的企图不能得逞。

(3) 通信双方互不信任，但对第三方(公证方)则绝对信任，于是依靠第三方来证实已发生的操作。

2. 支持安全服务的基本机制

为了实现上述五种安全服务，ISO 7498—2 中制定了支持安全服务的八种安全机制，安全机制与安全服务关系如表 1-2 所示：

表 1-2 OSI 安全服务与安全机制的关系

安全服务		安全机制							
		加密	数字签名	访问控制	数据完整性	认证	业务流填充	路由控制	公证
认证服务	对等实体认证	√	√			√			
	数据源认证	√	√						
访问控制服务	访问控制服务			√					
数据保密性	连接保密	√						√	
	无连接保密	√						√	
	选择字段保密	√							
	业务流保密	√					√	√	

续表

安全服务		安全机制							
		加密	数字签名	访问控制	数据完整性	认证	业务流填充	路由控制	公证
数据完整性	可恢复连接完整性	√			√				
	无恢复连接完整性	√			√				
	选择字段连接完整性	√			√				
	无连接完整性	√	√		√				
	选择字段无连接完整性	√	√		√				
防抵赖	源发方防抵赖		√		√				√
	接收方防抵赖		√		√				√

(1) 加密机制——是确保数据安全性的基本方法,在 OSI 安全体系结构中应根据加密所在的层次及加密对象的不同,而采用不同的加密方法。

(2) 数字签名机制——是确保数据真实性的基本方法,利用数字签名技术可进行用户的身份认证和消息认证,它具有解决收、发双方纠纷的能力。

(3) 访问控制机制——从计算机系统的处理能力方面对信息提供保护。当主体试图使用非授权资源或以不正确方式使用授权资源时,访问控制功能将拒绝这种企图并产生事件报警记录下来作为安全审计跟踪的一部分。

(4) 数据完整性机制——破坏数据完整性的主要因素有数据在信道中传输时受信道干扰影响而产生错误,数据在传输和存储过程中被非法入侵者篡改,计算机病毒对程序和数据的传染等。纠错编码和差错控制是防止信道干扰的有效方法。防止非法入侵者主动攻击的有效方法是保温认证,预防计算机病毒有各种病毒检测、杀毒和免疫方法。

(5) 认证交换机制——在计算机网络中认证主要有用户认证、消息认证、站点认证和进程认证等,可用于认证的方法有已知信息(如口令)、共享密钥、数字签名、生物特征(如指纹)等。认证交换技术的选择将依据它们被使用的环境而定。在通常情况下,它们要与时间戳和同步时钟、二次和三次握手、基于数字签名或公证机制的防抵赖服务等一起使用。

(6) 业务流填充机制——攻击者通过分析网络中某一路径上的信息流量和流向来判断某些事件的发生,为了对付这种攻击,一些关键站点间在无正常信息传送时,持续传递一些随机数据,使攻击者不知道哪些数据是有用的,哪些数据是无用的,从而挫败攻击者的信息流分析。

(7) 路由控制机制——在计算机网络中,从源点到目的地往往存在多条路径,其中有些路径是安全的,有些路径是不安全的。路由控制机制可根据信息发送者的申请选择安全路径,以确保数据安全。

(8) 公证机制——在计算机网络中,并不是所有的用户都是诚实可信的,同时也存在由于设备故障等技术原因造成信息丢失、延迟等情况,用户之间很可能引起责任纠纷,为了解

决这个问题，就需要有一个各方都信任的第三方以提供公证仲裁，仲裁数字签名技术是这种公正机制的一种技术支持。

ISO 安全体系结构针对的是基于 OSI 参考模型的网络通信系统，它所定义的安全服务也只是解决网络通信安全问题的技术措施，而系统安全、物理安全、人员安全等方面都没有涉及。ISO 体系关注的是静态的防护技术，它并没有考虑到信息安全动态性和生命周期性的发展特点，缺乏检测、响应和恢复等重要环节，因而无法满足更复杂更全面的信息保障要求。

1.3.2 P2DR 模型

P2DR 模型是美国 ISS 公司提出的动态网络安全体系的代表模型，也是动态安全模型的雏形。P2DR 模型包括四个主要部分：安全策略(Policy)、防护(Protection)、检测(Detection)和响应(Response)，如图 1-6 所示。



图 1-6 P2DR 模型示意图

1. 策略

安全策略具有一般性和普遍性，一个恰当的安全策略总会把关注的核心集中到最高决策层认为必须值得注意的那些方面。安全策略是模型的核心，所有的防护、检测和响应都是依据安全策略实施，安全策略为安全管理提供管理方向和支持手段。策略体系的建立包括安全策略的制定、评估与执行等。网络安全策略一般包括总体安全策略和具体安全策略两个部分。总体安全策略用于阐述本部门的信息网络安全的总体思想和指导原则，具体策略是根据总体策略提出的具体实施规则，说明哪些行为是允许的，哪些行为是被禁止的。

2. 防护

防护是根据系统可能出现的安全问题而采取的一切预防措施，预先阻止攻击条件的产生，让攻击者无法顺利地入侵。所以说，防护是网络安全策略中最重要的环节。防护措施一般与传统的静态安全技术相结合，安全技术通常包括数据加密、身份认证、访问控制、授权和虚拟专用网(VPN)技术、防火墙、安全扫描和数据备份等。

防护分为三大类：系统安全防护、网络安全防护和信息安全防护。系统安全防护指的是操作系统的安全防护，即各个操作系统的安全配置、使用和打补丁等。不同操作系统有不同的防护措施和相应的安全工具。网络安全防护指的是网络管理的安全，以及网络传输的安全。通过防火墙监视、限制进出网络的数据包，防范内外网之间的非法访问，提高网络的防护能力。信息安全防护指的是数据本身的保密性、完整性和可用性。数据加密就是信息安全防护的重要技术。

3. 检测

利用检测工具如漏洞评估、入侵检测系统来了解判断网络系统的安全状态。当攻击者

穿透防护系统时，检测功能就发挥作用，与防护系统形成互补。检测是动态响应的依据，在网络安全循环过程中，它是非常重要的一个环节，帮助系统有效对付网络攻击，增强网络安全管理能力，提高信息安全基础结构的完整性，是整个模型动态性的体现。

检测的对象主要针对系统自身的脆弱性及外部威胁。主要包括：检查系统存在的脆弱性；在计算机系统运行过程中，检查、测试信息是否发生泄露、系统是否遭到入侵，并找出泄露的原因和攻击的来源。如计算机网络入侵检测、信息传输检查、电子邮件监视、电磁泄露辐射检测、屏蔽效果测试、磁介质消磁效果验证等。

4. 响应

响应是解决安全潜在性的最有效的方法，系统一旦检测到安全漏洞和安全事件，响应系统就开始工作。响应系统及时进行事件处理，杜绝危害进一步扩大，将网络系统的安全性调整到风险最低的状态，使系统提供正常的服务。响应包括紧急响应和恢复处理，恢复处理又包括系统恢复和信息恢复。

P2DR 模型是在整体安全策略的控制和指导下，在综合运用防护工具（如防火墙、操作系统身份认证、加密等）的同时，利用检测工具（如漏洞评估、入侵检测等）了解和评估系统的安全状态，通过适当的反应将系统调整到“最安全”和“风险最低”的状态。防护、检测和响应组成了一个完整的、动态的安全循环，在安全策略的指导下保证信息系统的安全。也就是说，系统的安全实际上是理想中的安全策略和实际的执行之间的平衡，强调在防护、监控检测、响应等环节的循环过程，通过这种循环达到保持安全水平的目的。所以，P2DR 安全模型是整体的、动态的安全模型，应该依据不同等级的系统安全要求来完善系统的安全功能、安全机制。模型给出了一个全新的安全定义：“及时的检测和响应就是安全”或者“及时的检测和恢复就是安全”。

P2DR 模型也存在一个明显的弱点，即忽略了内在的变化因素，如人员的流动、人员的素质和策略贯彻的不稳定性。实际上，安全问题牵涉面广，除了涉及防护、检测和响应，系统本身安全的“免疫力”的增强、系统和整个网络的优化，以及人员这个在系统中最重要角色的素质的提升，都是该安全系统没有考虑到的问题。

1.3.3　WPDRRC 模型

进入 20 世纪 90 年代，信息网络系统的攻击事件日趋频繁，对信息及信息网络系统单纯的保护已不能满足安全的需要，美国国家安全局在发布的《信息保障技术框架》中提出了深层防御的安全设计思想：从宏观上提出了人、政策（包括法律、法规、制度、管理）和技术三大要素来构成宏观的信息网络安全保障体系结构的框架。

信息网络安全保障不仅仅是技术问题，而是人、政策和技术三大要素的结合。人是在最底层，是信息网络安全管理的根本。保障信息网络系统的安全性，既要靠先进的技术，又要有完善的管理，但其核心都是人，实际上，大部分安全和保密问题是由人为差错造成的。因此，在信息网络安全管理中人的因素应该是最重要的。它主要包括人员的岗位责任安全、人

事监督监测、安全保密协议、安全事件及隐患报告、安全教育与培训、安全奖惩制度等，另外，还要有和组织外部的合作者进行信息交流时的安全性规定。技术是顶端的东西，但是技术是要通过人，通过相应的政策和策略去操作这个技术的。

总的来说，人是核心，政策是桥梁，技术是保证。人通过政策将技术落实在 WPDRRC 六个环节的各个方面。

(1) 预警(Warning)：根据以前掌握系统的脆弱性和了解当前的犯罪趋势，预测未来可能受到的攻击和危害。

(2) 保护(Protection)：采用一切手段保护信息系统的保密性、完整性、可用性、可控性和不可否认性。

(3) 检测(Detection)：检测本地网络的安全漏洞和存在的非法信息流，从而有效阻止网络攻击。

(4) 响应(Respond)：对危及网络安全的事件和行为做出反应，阻止对信息系统的进一步破坏并使损失降到最低。

(5) 恢复(Restore)：及时恢复系统，使其尽快正常对外提供服务，是降低网络攻击造成损失的有效途径。

(6) 反击(Counterattack)：采用一切可能的高新技术手段，侦察、提取计算机犯罪分子的作案线索与犯罪证据，形成强有力的取证能力和依法打击手段。

WPDRRC 安全体系模型不仅包含安全防护的概念，更重要的是增加了主动和积极的防御观念。

网络安全实际上是一项系统工程，它涉及的方方面面都不可忽视。信息网络安全遵循“木桶原则”，即一个木桶的容积决定于它最短的一块木板，一个系统的安全强度等于它最薄弱环节的安全强度。无论采用了多么先进的设备，如果安全管理上有漏洞，那么这个系统的安全一样没有保障。在网络安全管理中，专家们一致认为是“三分技术，七分管理”。同时，网络安全不是一个目标，而是一个过程，而且是一个动态的过程，因为制约安全的因素都是动态变化的，必须通过一个动态的过程来保证安全。安全是相对的，所谓安全，实际上是根据客户的实际情况，在实用性和安全性之间找一个平衡点。

1.4 信息网络安全的策略

信息网络安全策略确定网络安全保护工作的目标和对象。信息网络安全策略涵盖面很广，如总体安全策略、网络安全策略、应用系统安全策略、部门安全策略、设备安全策略等。一个信息系统的总体安全策略，就是要保证信息系统“实体可信，行为可控，资源可管，事件可查，运行可靠”。

实体可信即保证构建网络的基础设备和软件系统安全可信，没有预留后门或逻辑炸弹。保证接入网络的用户是可信的，防止恶意用户对系统的攻击破坏。保证在网络上传输、处

理、存储的数据是可信的,防止搭线窃听,非授权访问或恶意篡改。

行为可控即保证本地计算机的各种软硬件资源不被非授权使用或被用于危害本系统或其他系统的安全。保证网络接入可控,用户上网必须申请登记并得到许可。保证网络行为可控,即保证网络上的通信行为受到监视和控制,防止滥用资源、非法外联、网络攻击、非法访问和传播有害信息等恶意事件的发生。

资源可管即保证对路由器、交换机、服务器、邮件系统、目录系统、数据库、域名系统、安全设备、密码设备、密钥参数、交换机端口、IP 地址、用户账号、服务端口等网络资源进行统一管理。

事件可查即保证对网络上的各类违规事件进行监控记录,确保日志记录的完整性,为安全事件稽查、取证提供依据。

运行可靠即保证网络节点在发生自然灾难或遭到硬摧毁时仍能不间断运行,具有容灾抗毁和备份恢复能力。保证能够有效防范病毒和黑客攻击所引起的网络拥塞、系统崩溃和数据丢失,并具有较强的应急响应和灾难恢复能力。

1.4.1 信息网络安全管理

信息网络安全的复杂性、多变性和信息系统的脆弱性决定了信息网络安全问题是必然存在的。在日常的工作生活中,需更多地依靠管理策略来保证信息网络的安全。

1. 信息网络安全管理的特点

1) 信息网络安全管理的必然性

随着国际政治形势的发展以及经济全球化的加快,信息网络安全问题不仅涉及国家的经济安全、金融安全,也涉及国家的国防安全、政治安全和文化安全。因此,在信息社会中,没有对信息安全的管理是不可想象的。正如前节所述,信息网络安全是人、政策和技术三大要素的结合,管理是和日常工作生活关系最为紧密的安全保障手段。

2) 信息网络安全管理代价的相对性

加强信息网络安全管理需要安全管理人员,管理机构,制定管理制度。这些都需要花费一定的社会资源和代价,而这个代价如果超出了要保护的信息网络系统的价值,则是不合适的。管理的代价和保护的资源的价值总是处于一种相对平衡状态。

3) 信息网络安全管理的动态性

信息网络安全威胁总是随着社会的发展和技术的进步在不断变化,由于新技术的产生和新产品的出现,新的安全威胁也在不断地出现。对于新的安全威胁要采用新的安全管理措施和制度来加以防范,不能指望一项技术或措施一劳永逸地保护所有信息网络资源的安全,必须动态地持续地保护信息网络资源。

4) 信息网络安全管理的广泛性

随着社会信息化程度的不断提高,信息网络系统在社会生活的方方面面都有涉及,有信息网络系统就需要网络安全管理。

5）信息网络安全管理的黑盒性

信息网络安全防护是一种“防患于未然”为特征的安全防护，一种安全防护措施不像其他系统那样明确公开，一般都比较模糊。如防火墙能防御哪些攻击，一般是不好确定的。因此，对安全产品的鉴定、评价和认证就显得特别重要，国际上的各种认证机构如国际计算机安全协会及我国公安部网络安全检测中心等第三方中介机构对于安全产品的认证和评价就显得比较有意义。

2. 信息网络安全立法

信息网络安全是人类当今遭遇的最大安全，它既是一个全新的安全，也是一个最大的安全。因为信息安全不仅涉及用户、企业、政府，还涉及政治、经济、军事等因素，包括了人身安全、财产安全、社会安全、国家安全、网络安全，涉及了整个社会的几乎所有因素。法律是国家意志的体现，是一种制度保障和行为约束，要维护社会和谐，维护每一个人的权益。信息网络安全法律法规是信息网络领域的专门法律，它具有两方面的作用：一方面在信息网络安全领域它是人们的行为规范，对网络犯罪具有预防作用；另一方面它以强制力为后盾，为信息网络安全构造最后一道防线，如果违反了信息网络安全法规就要承担相应的法律责任，受到法律的惩处。

1）各国政府信息安全的立法

随着信息网络的迅猛发展，世界各国都比较注重信息网络安全方面的立法工作，希望通过法律来加强对信息网络安全的保护。

（1）美国。

1987 年就通过了《计算机安全法》，该法确立了计算机服务盗窃罪、侵犯知识产权罪、破坏计算机设备或配置罪、计算机诈骗罪、通过欺骗获得电话或电报服务罪、计算机滥用罪、计算机错误访问罪、非授权的计算机使用罪等罪名。与别的国家相比，美国无疑是信息安全方面的法案最多，而且较为完善的国家。

（2）英国。

1996 年 9 月 23 日，英国政府颁布了第一个网络监管行业性法规《三 R 安全规则》。“三 R”分别代表分级认定、举报告发、承担责任。法规旨在从网络上消除儿童色情内容和其他有害信息，对提供网络服务的机构、终端用户和编发信息的网络新闻组，尤其是对网络提供者做出了明确的责任分工。2000 年英国政府又公布了新的《通信法案》的征求意见稿。这一草案酝酿已久，其主要目的是促进英国电子商务发展，并为社会各界树立对电子商务的信心，提供法律上的保障。

（3）俄罗斯。

俄罗斯于 1995 年颁布了《联邦信息、信息化和信息保护法》。该法强调了国家建立信息资源和信息化中的责任是“旨在为完成俄联邦社会和经济发展的战略、战役服务，提供高效率高质量的信息保障创造条件”。法规中明确界定了信息资源开发和保密范畴，提出了保护信息的法律责任。

2）国际公约

2004 年 7 月 1 日生效的欧洲理事会《关于网络犯罪的公约》(以下简称《公约》)是打击网络犯罪的第一个国际公约，其主要目标是在缔约方之间建立打击网络犯罪的共同的刑事政策、一致的法律体系和国际协助。《公约》除序言外，正文分为四章，共计 48 个条文。由于《公约》是目前签署方最多的生效开放性国际公约，因此该公约建立的电子证据跨国刑事调查的国际法律机制最具国际影响力。

3. 我国的信息网络安全立法

伴随着信息网络技术的发展，我国对信息网络安全的立法工作就一直没有中断过。1994 年 2 月 18 日，国务院发布了第 147 号令《中华人民共和国计算机信息安全保护条例》，这是我国第一部有关信息网络安全管理的法律法规。该条例的发布，意味着我国的网络信息安全进入了有法可依的阶段，我国的信息网络安全立法也开始步入轨道。紧接着，国家和地方政府以及行业主管部门相继颁布实施了一系列信息网络安全方面的法律法规、规章及公约，初步形成了具有中国特色的包括宪法、法律、法规、行政部门规章、司法解释等多层面的信息网络安全法律体系。

4. 信息网络安全监督管理

信息网络安全监督管理工作既包括公共信息网络安全保卫部门依照法律法规对互联网单位的备案、互联网运营单位、互联网信息服务单位以及联网单位的监督、检查、管理工作，也包括公安机关网络安全保卫部门依法对重要信息系统的监督、指导工作。主要包括：指导督促互联网单位的备案工作；监督、检查互联网单位落实安全管理制度和安全保护技术措施；监督管理互联网上网服务营业场所，严格进行安全审核和日常检查。同时还包括互联网有害信息、信息网络违法违规行为的监督查处，组织开展计算机病毒等破坏性程序的日常防治管理以及计算机安全员培训与管理等。

5. 互联网信息内容安全管理

目前互联网的海量信息，给人们的工作、学习、生活带来极大便利，也给人们带来相当大的"信息冲击"，由此产生诸多信息内容安全问题，互联网信息内容安全管理包括：境外敌对势力、宗教极端势力、邪教组织等利用互联网向境内进行渗透煽动、破坏活动的问题；利用主页、电子公告栏、留言板、聊天室、微博等交互式栏目张贴、传播有害信息，泄露国家秘密的问题；利用电子邮件和短信息发送有害信息的问题；对有害信息不防范、不删除、不报告，管理失控的问题；利用 IP 电话、手机短信息、声讯服务等渠道传播有害信息的问题；利用互联网进行诈骗、盗窃、赌博等违法活动的问题；利用互联网提供的搜索引擎查找、链接各种有害信息的问题等。全面清理网上有害信息，实现互联网热点信息管理，已经成为信息网络安全管理工作的一项重要任务。

6. 互联网上网服务营业场所安全管理

目前，互联网上网服务营业场所安全管理的对象主要是网吧。网吧应落实信息安全管理措施和信息安全技术措施来完善网吧的信息网络安全。上网者在网吧接触、传播有害信

息始终是管理部门监管的重点，经营单位和上网消费者不得利用互联网上网服务营业场所制作、下载、复制、查阅、发布、传播或者以其他方式使用有害信息，不得进行制作或者传播计算机病毒等危害信息网络安全的活动。经营单位应当对上网消费者的身份证等有效证件进行核对、登记，并记录有关上网信息，经营单位还应当实施经营管理技术措施，建立场内巡查制度，发现上述行为，应当立即予以制止并向文化行政部门、公安机关举报。管理部门应当采取其他有效办法以维护网络安全。同时经营单位应当通过依法取得经营许可证的互联网接入服务提供者接入互联网，不得采取其他方式接入互联网，经营单位提供上网消费者使用的计算机必须通过局域网的方式接入互联网，不得直接接入互联网。这样就从技术层面减少消费者接触有害信息的可能性。

网吧的安全管理人员、经营管理人员、专业技术人员参加安全培训是国家的法定要求。公安机关要求：新开办网吧必须有两名以上安全管理人员、专业技术人员取得培训合格证。

7. 信息安全等级保护管理

目前国内外各种势力对我们国家的重要信息系统和基础网络进行入侵、攻击、破坏，给国家安全带来严重威胁；同时国内信息网络违法犯罪日益猖獗，数量持续上升；我国现有基础信息网络和重要信息系统安全建设基础已完成但还存在隐患严重。

我国借鉴了西方发达国家对于国家关键基础设施保护的思路、策略和方法。创建出符合中国国情的信息安全等级保护制度。信息安全等级保护是国家信息安全保障工作的基本制度，是我们国家的信息安全保障的政策体系。将国家有限的财力、物力、人力投入到重要信息系统安全保护中，有效保护基础信息网络和关系国家安全、经济命脉、社会稳定的重要信息系统，有效提高我国信息安全保障工作的整体水平。信息安全等级保护不仅体现在信息系统的整个生命周期，还要从技术和管理两方面进行安全建设。公安机关要为开展好这项工作提供服务和保障，进行监督、检查和指导。

通过开展等级保护，各单位、各部门首先对自己的信息网络和信息系统进行调查摸底，然后开展定级、备案、安全建设整改、等级测评、安全检查等工作，基础网络和重要信息系统结合开展风险评估、灾难备份、应急处置、安全监控等工作，找到了开展信息安全保障工作的有效方法。国家通过制定统一的管理规范和技术标准，组织行政机关、公民、法人和其他组织根据信息和信息系统的不同重要程度开展有针对性的保护工作。

1.4.2 信息网络安全技术

信息网络安全是一项系统工程，针对来自不同方面的安全威胁，需要采取不同的安全对策。从法律、制度、管理和技术上采取综合措施，以便相互补充，达到较好的安全效果。技术措施是最直接的屏障，目前常用而有效的信息网络安全技术策略有如下几种。

1. 加密技术

加密技术包括两个元素：算法和密钥。算法是将普通的文本与一串数字（密钥）结合，产生不可理解的密文的步骤；密钥是用来对数据进行编码和解码的一种算法。在安全保密

中,可通过适当的密钥加密技术和管理机制来保证网络的信息通讯安全。密钥加密技术的密码体制分为对称密钥体制和非对称密钥体制两种。相应地,对数据加密的技术分为两类,即对称加密和非对称加密。对称加密的加密密钥和解密密钥相同,而非对称加密的加密密钥和解密密钥不同,加密密钥可以公开而解密密钥需要保密。加密算法多种多样,在信息网络中一般是利用信息变换规则把明文的信息变成密文的信息。攻击者即使得到经过加密的信息,也不过是一串毫无意义的字符。加密可以有效地对抗截收、非法访问等威胁。加密算法可以分为对称加密、非对称加密和哈希算法三类。

对称加密算法:加密密钥和解密密钥相同或者可以由其中一个推知另一个,通常把参与加密、解密过程的相同的密钥叫做公共密钥。代表性的对称式加密算法有 DES(数据加密标准)、IDEA(国际数据加密算法)、Rijndael、AES、RC4 算法等。

非对称加密算法。加密和解密使用不同的密钥,每个用户拥有一对密钥,其中的一个作为公钥,公钥是公开的,任何人都可以获得;另一个作为私钥,私钥是保密的,只有密钥对的拥有者独自知道。在使用过程中一个用来加密,另一个一定能够进行解密。典型的非对称加密算法有 RSA、DSA 等。

哈希算法,也称为单向散列函数、杂凑函数、HASH 算法或消息摘要算法。它通过一个单向数学函数,将任意长度的一块数据转换为一个定长的、不可逆转的数据。这段数据通常叫做消息摘要,其实现过程通常称为压缩。典型的哈希算法有 MD5、SHA、HMAC、GOST 等。

2. 身份认证技术

身份认证技术是在计算机网络中为了确认操作者身份而产生的解决方法。计算机网络世界中一切信息包括用户的身份信息都是用一组特定的数据来表示的,计算机只能识别用户的数字身份,所有对用户的授权也是针对用户数字身份的授权。如何保证以数字身份进行操作的操作者就是这个数字身份合法拥有者,也就是说保证操作者的物理身份与数字身份相对应,身份认证技术就是为了解决这个问题,作为防护网络资产的第一道关口,身份认证有着举足轻重的作用。

在信息网络安全中经常使用的身份认证手段有:静态密码、智能卡(IC 卡)、短信密码、动态口令牌、USB KEY、数字签名、生物识别。

3. 虚拟专用网技术

虚拟专用网(VPN)被定义为通过一个公用网络(如因特网)建立一个临时的、安全的连接,是一条穿过公用网络的安全、稳定的隧道。使用这条隧道可以对数据进行几倍加密达到安全使用互联网的目的。虚拟专用网是对企业内部网的扩展,可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接,并保证数据的安全传输。虚拟专用网可用于不断增长的移动用户的全球因特网接入,以实现安全连接;可用于实现企业网站之间安全通信的虚拟专用线路。

VPN 可以提供的功能有数据加密、数据完整性、数据源认证和防重放。VPN 有三种解

决方案,即远程访问虚拟网、企业内部虚拟网和企业扩展虚拟网。

4. 防火墙技术

防火墙技术,最初是针对 Internet 网络中的不安全因素所采取的一种保护措施,是用来阻挡外部不安全因素影响的内部网络屏障,其目的就是防止外部网络用户未经授权的访问。它是一种计算机硬件和软件的结合,使 Internet 与 Intranet 之间建立起一个安全网关,从而保护内部网免受非法用户的侵入。防火墙主要由服务访问政策、验证工具、包过滤和应用网关 4 个部分组成。

5. 入侵检测技术

入侵检测技术是网络安全研究的一个热点,是一种积极主动的安全防护技术,提供了对内部入侵、外部入侵和误操作的实时保护,在网络系统受到危害之前拦截相应入侵。随着时代的发展,入侵检测技术将朝着三个方向发展:分布式入侵检测、智能化入侵检测和全面的安全防御方案。

进行入侵检测的软件与硬件的组合就是入侵检测系统,它主要是完成检测的功能,除此之外还有如下功能:检测部分阻止不了的入侵;检测入侵的前兆,从而加以处理,如阻止、封闭等;入侵事件的归档,从而提供法律依据;网络遭受威胁程度的评估和入侵事件的恢复。入侵检测系统根据信息源的不同可分为基于主机的入侵检测系统(HIDS)和基于网络的入侵检测系统(NIDS)。

6. 安全扫描技术

安全扫描技术也称为脆弱性评估技术,采用模拟黑客攻击的方式对目标可能存在的已知安全漏洞进行逐项检测,以便对工作站、服务器、交换机、数据库等各种对象进行安全漏洞检测。

安全扫描技术按扫描的主体分为基于主机的安全扫描技术和基于网络的安全扫描技术。按扫描过程分为 ping 扫描技术、端口扫描技术、操作系统探测扫描技术、已知漏洞的扫描技术。

7. 数据备份与恢复技术

计算机系统经常会因各种原因不能正常工作,会损坏或丢失数据,甚至出现整个系统崩溃的情况。一般通过备份技术保留用户甚至整个系统数据,当系统不正常时可以通过该备份恢复工作环境。

数据备份有多种方式,在不同情况下,应该选择最合适的方法。按备份的数据量来划分有完全备份、增量备份、差分备份和按需备份。按备份的状态来划分有物理备份和逻辑备份。按备份的地点来划分有本地备份和异地备份。

8. 病毒防护技术

计算机病毒是对信息网络安全威胁比较大的因素之一,它也随着信息技术的进步在不断地发展着,从最初的单机间通过存储介质相互传播,发展到今天的多种渠道传播,如 E-mail 传播、即时通信工具传播、无线信道传播等。其破坏性越来越大,由最初的破坏文件数

据，发展到今天的破坏信息系统、使网络瘫痪，甚至盗窃用户账户中的钱财。用户可通过病毒防护技术来减少病毒、间谍软件和恶意软件带来的风险和危害。

习　　题

1. 简述信息网络系统的五个安全特性。
2. P2DR 模型中的 P、P、D、R 的含义是什么？
3. 信息网络安全的策略包括哪些内容？
4. 信息网络安全管理的主要内涵是什么？

第 2 章

信息网络安全法律法规

【内容提要】

本章介绍了我国信息网络安全法律法规体系的构成与建设过程。通过学习，要求学生了解信息网络安全相关法律法规与部门规范。

信息网络安全法律法规作为国家法律体系的重要组成部分之一，在维护和保障信息网络安全中占有举足轻重的地位。近年来，对于信息网络安全保障工作我们应该以管理和技术并重的角度来维护安全。同时，努力加强信息网络安全立法工作，完善信息网络安全法律体系，加大法律执行力度，才能有效的保障信息网络安全；信息网络安全法律法规是信息网络安全保障体系建设中的必要环节，它明确信息网络安全的基本原则和基本制度、信息网络安全相关行为的规范、信息网络安全中各方权利和义务、违反信息网络安全的行为，并明确对其行为进行相应的处罚。信息网络安全立法能够保护国家信息主权和社会公共利益，规范信息活动，保护信息权利，协调和解决信息网络社会产生的矛盾，打击、惩治信息网络空间的违法行为，同时依托信息网络安全的司法和执法来实施法定程序和法律活动。

2.1　信息网络安全法律法规体系

法律是保障信息网络安全的一道利器。近年来我国在信息网络安全领域的法制建设方面做了大量工作，但相对于信息网络技术的迅猛发展及其在经济社会生活各方面日益显著的作用，信息网络安全立法工作滞后和不完善的问题也日益突出。因此，应当充分认识加强信息网络安全立法的紧迫性、重要性，抓紧建立和完善国家信息网络安全法律框架。

2.1.1　信息网络安全法律法规概述

没有规矩，不成方圆。法律法规是指国家按照统治阶级的利益和意志制定、认可，并由国家强制力保障其实施的行为规范的总和，是人们在社会活动中必须遵守的纪律，是人们从事社会活动所不能逾越的行为底线，违犯了就要受到惩罚。

信息网络安全关乎国家安全和社会稳定，信息网络安全发展状况与相关“规矩”的不断

建立和完善分不开。这些“规矩”大致可分成法律、法规、标准等部分。

信息网络安全法律法规是所有相关信息网络安全法律法规的总和。主要包括命令性和禁止性规范两种。一般命令性规范要求法律关系的主体(法律关系的主体主要包括公民、各种国家机构和部门、国家)应当或必须从事一定的行为；禁止性规范则要求法律关系的主体不得从事指定的行为，否则就要受到一定的法律法规制裁。

2.1.2　我国信息网络安全法律法规

1. 信息网络安全法律法规发展

我国的法律体系是由以宪法为核心的各个法律部门所组成，作为维护信息网络安全与秩序的信息网络安全法律规范是一个不可缺少的法律部分，其为保证信息网络稳步、健康发展，保障整个社会环境的稳定发挥了重要作用。同时国家、地方以及相关部门针对信息网络安全的需求，制定了一系列与信息网络安全相关的法律法规。从领域上看，涉及网络与信息系统安全、信息内容安全、信息安全系统与产品、保密及密码管理、计算机病毒与危害性程序防治、金融、证券、教育等特定领域的信息安全、信息网络安全犯罪制裁等多个方面；从形式上看，有法律、行政法规、部门规章规范、相关的决定、司法解释及相关文件、地方性法规与地方政府规章及相关文件等多个层次。

与此同时，与信息网络安全相关的司法和行政管理体系逐渐在完善，信息网络安全法律体系已初步建立，但整体来看，与美国、欧盟等先进国家与地区比较，我国在信息网络安全相关法律法规方面还欠体系化、有效性、覆盖面与深度，缺乏相关的基本法，信息网络安全法律法规的建设与发达国家还有一定差距。

2. 信息网络安全法律法规体系构成

我国信息网络安全的保护主要通过以下两个方面的法律法规予以保障。

1) 信息网络安全国家法律

国家在许多基本法律中都设计了用于保护信息网络安全的条款，在《中华人民共和国宪法》、《中华人民共和国刑法》、《中华人民共和国国家安全法》、《中华人民共和国反不正当竞争法》、《中华人民共和国警察法》、《中华人民共和国预防未成年人犯罪法》、《全国人大常委会关于维护互联网安全的决定》、《中华人民共和国证券投资基金法》、《 中华人民共和国电子签名法》、《 中华人民共和国证券法》、《中华人民共和国治安管理处罚法》、《中华人民共和国突发事件应对法》、《中华人民共和国侵权责任法》、《中华人民共和国著作权法》、《中华人民共和国保守国家秘密法》等国家法律法规中都针对信息网络安全的保护做出了相关的明确规定。

2) 信息网络安全行政法规与部门规范

国务院、国务院管辖部门、国务院直属机构也依据自身行业的特点与应用有针对性地出台了与有关行业、部门的信息网络安全保护相关的行政法规和部门规范。

3. 信息网络安全法律法规作用

(1) 指引作用：是指法律法规作为一种行为规范，为人们提供了某种行为模式，指引人们可以的行为方式，告诉人们必须这样行为和不能那样行为的规范。

(2) 评价作用：是指法律具有判断、衡量人们行为是否合法或违法，并能够确定违法行为的性质以及针对这些违法行为所承担的责任。

(3) 预测作用：是指人们可以根据法律预先估计到自身应该如何行为以及其违法行为在法律上的后果。

(4) 教育作用：是指通过法律的实施对一般人今后的行为产生警示和教育影响。

(5) 强制作用：是指法律对违法行为具有制裁、惩罚的作用。

2.2 信息网络安全法律法规与部门规范

信息网络安全法律法规体系构成中指出我国信息网络安全法律法规主要包括信息网络安全国家法律、信息网络安全行政法规和信息网络安全部门规范等多种形式。

2.2.1 信息网络安全相关国家法律

信息网络安全相关国家法律主要指全国人民代表大会和全国人民代表大会常务委员会审议通过的国家法律法规。

由全国人民代表大会审议通过的法律法规解释如下：

- 《中华人民共和国宪法》(2004 年 3 月 14 日第十届全国人民代表大会第二次会议通过的《中华人民共和国宪法修正案》)中明确了中华人民共和国公民在保障我国信息网络安全中的责任和义务。
- 《中华人民共和国刑法》(2011 年 2 月 25 日中华人民共和国第十一届全国人民代表大会常务委员会第十九次会议通过《中华人民共和国刑法修正案》(八))中明确了针对危害国家安全，危害公共安全，破坏社会主义市场经济秩序，侵犯公民人身权利、民主权利，侵犯财产，妨害社会管理秩序，危害国防利益，渎职，军人违反职责等诸多与信息网络安全内容相关的刑罚。

由全国人民代表大会常务委员会审议通过的法律法规解释如下：

- 《中华人民共和国国家安全法》(1993 年 2 月 22 日第七届全国人民代表大会常务委员会第三十次会议通过，2009 年 8 月 27 日根据《全国人民代表大会常务委员会关于修改部分法律的决定》修订)是为了维护国家安全，保卫中华人民共和国人民民主专政的政权和社会主义制度，保障改革开放和社会主义现代化建设的顺利进行，根据宪法制定的一部法律；法律中明确了公民维护国家安全的责任和义务的同时，对国家安全机关在国家安全工作中的职权，公民和组织维护国家安全的义务和权利方面都有与信息网络安全相关的法规与相应的法律责任。

- 《中华人民共和国反不正当竞争法》(1993 年 9 月 2 日第八届全国人民代表大会常务委员会第三次会议通过)是为保障社会主义市场经济健康发展，鼓励和保护公平竞争，制止不正当竞争行为，保护经营者和消费者的合法权益制定的一部法律；法律中明确了哪些是与信息网络安全相关的不正当竞争行为，并指出相应的监督检查职权与法律责任。
- 《中华人民共和国警察法》(1995 年 2 月 28 日第八届全国人民代表大会常务委员会第十二次会议通过)是为了维护国家安全和社会治安秩序，保护公民的合法权益，加强人民警察的队伍建设，从严治警，提高人民警察的素质，保障人民警察依法行使职权，保障改革开放和社会主义现代化建设的顺利进行，根据宪法制定的一部法律，法律中明确了中国人民警察的职责分工。
- 《中华人民共和国预防未成年人犯罪法》(1999 年 6 月 28 日中华人民共和国第九届全国人民代表大会常务委员会第十次会议通过) 是为了保障未成年人身心健康，培养未成年人良好品行，有效地预防未成年人犯罪而制定的一部法律；法律中明确了未成年人在接触和使用与信息网络安全内容相关的行为和处罚规定。
- 《全国人大常委会关于维护互联网安全的决定》(2000 年 12 月 28 日第九届全国人民代表大会常务委员会第十九次会议通过)是为保障互联网的运行安全和信息网络安全问题，促进我国互联网的健康发展，维护国家安全和社会公共利益，保护个人、法人和其他组织的合法权益而制定的法规，法规中界定了互联网安全方面的行为及其刑事责任。
- 《中华人民共和国证券投资基金法》(2003 年 10 月 28 日第十届全国人民代表大会常务委员会第五次会议通过)是为了规范证券投资基金活动，保护投资人及相关当事人的合法权益，促进证券投资基金和证券市场的健康发展，制定的法规。法规中明确了基金的运作与信息披露中与信息网络安全内容相关的违规行为与法律责任。
- 《中华人民共和国电子签名法》(2004 年 8 月 28 日第十届全国人民代表大会常务委员会第十一次会议通过)是为了规范电子签名行为，确立电子签名的法律效力，维护有关各方的合法权益，制定的一部法规，法规中明确了数据电文，电子签名与认证等与信息网络安全内容相关的行为。
- 《中华人民共和国证券法》(2005 年 10 月 27 日第十届全国人民代表大会常务委员会第十八次会议修订)为了规范证券发行和交易行为，保护投资者的合法权益，维护社会经济秩序和社会公共利益，促进社会主义市场经济的发展，制定的一部法规，法规中明确了证券交易，证券公司，证券登记结算机构，证券服务机构，证券监督管理机构等证券交易活动与部门行为的法律责任。
- 《中华人民共和国治安管理处罚法》(2005 年 8 月 28 日第十届全国人民代表大会常务委员会第十七次会议通过)是为维护社会治安秩序，保障公共安全，保护公民、法人和其他组织的合法权益，规范和保障公安机关及其人民警察依法履行治安管理职

责，制定的一部法律；法律中明确了与信息网络安全内容相关违法行为的治安处罚。

- 《中华人民共和国突发事件应对法》(2007 年 8 月 30 日中华人民共和国第十届全国人民代表大会常务委员会第二十九次会议通过)是为了预防和减少突发事件的发生，控制、减轻和消除突发事件引起的严重社会危害，规范突发事件应对活动，保护人民生命财产安全，维护国家安全、公共安全、环境安全和社会秩序，制定的一部法规，法规中明确了针对我国突发事件应对过程中预防与应急准备，监测与预警，应急处置与救援，事后恢复与重建等涉及信息网络安全内容的行为与法律责任。
- 《中华人民共和国侵权责任法》(2009 年 12 月 26 日中华人民共和国第十一届全国人民代表大会常务委员会第十二次会议通过)是为保护民事主体的合法权益，明确侵权责任，预防并制裁侵权行为，促进社会和谐稳定制定的一部法规；法规中明确了网络用户、网络服务提供者利用网络侵害他人民事权益时应用承担侵权责任的具体规定。
- 《中华人民共和国著作权法》(2010 年 2 月 26 日第十一届全国人民代表大会常务委员会第十三次会议获得通过中华人民共和国著作权法修正)为保护文学、艺术和科学作品作者的著作权，以及与著作权有关的权益，鼓励有益于社会主义精神文明、物质文明建设的作品的创作和传播，促进社会主义文化和科学事业的发展与繁荣，根据宪法制定的一部法规。法规中明确了著作权，出版、表演、录音录像、播放等与信息网络安全内容相关的行为与法律责任和执法措施。
- 《中华人民共和国保守国家秘密法》(2010 年 4 月 29 日第十一届全国人民代表大会常务委员会第十四次会议修订)是为了保守国家秘密，维护国家安全和利益，保障改革开放和社会主义建设事业的顺利进行，制定的一部法律。法律中明确了针对国家秘密的范围和密级，保密制度，监督管理等方面与信息网络安全内容相关的行为与法律责任。

2.2.2 信息网络安全相关行政法规

由国务院通过的行政法规的解释如下：

- 《中华人民共和国计算机信息系统安全保护条例》(1994 年 2 月 18 日中华人民共和国主席令第 147 号)是为了保护计算机信息系统的安全，促进计算机的应用和发展，保障社会主义现代化建设的顺利进行制定的；条例中界定了计算机信息系统的概念，明确了安全保护工作的性质，计算机信息系统安全保护工作的重点，安全监督的职权和义务，信息系统设置的安全保护制度，并规定了违法者的法律责任。
- 《中华人民共和国计算机信息网络国际联网管理暂行规定》(1997 年 5 月 20 日中华人民共和国主席令 218 号)是为了加强对计算机信息网络国际联网的管理，保障国

际计算机信息交流的健康发展制定的，规定中明确了公安机关的职责和义务，规定了相关部门、单位和个人在计算机信息网络国际联网安全保护方面的责任以及在计算机网络国际联网安全保护方面违法的法律责任。

- 《商用密码管理条例》(1999 年 10 月 7 日中华人民共和国国务院令 273 号)是为了加强商用密码管理，保护信息安全，保护公民和组织的合法权益，维护国家的安全和利益制定的；条例中明确了商用密码的科研、生产管理，销售管理，使用管理，安全、保密管理等内容，并规定了相应的罚则。
- 《中华人民共和国电信条例》(2000 年 9 月 25 日国务院 31 次常务会议通过，中华人民共和国国务院令第 291 号)是为了规范电信市场秩序，维护电信用户和电信业务经营者的合法权益，保障电信网络和信息的安全，促进电信业的健康发展制定的；条例中明确了电信市场中相应的电信业务许可、电信网间互联、电信资费、电信资源，电信服务，电信建设中电信设施建设、电信设备进网，电信安全等内容，并规定了相应的罚则。
- 《互联网信息服务管理办法》(2000 年 9 月 20 日国务院 31 次常务会议通过，中华人民共和国国务院令第 292 号)是为了规范互联网信息服务活动，促进互联网信息服务健康有序发展制定的；办法中明确了互联网向上网用户提供信息的服务活动的一系列行为规定。
- 《计算机软件保护条例》(2001 年 12 月 20 日中华人民共和国主席令第 339 号)是为了保护计算机软件著作权人的权益，调整计算机软件在开发、传播和使用中发生的利益关系，鼓励计算机软件的开发与应用，促进软件产业和国民经济信息化的发展，根据《中华人民共和国著作权法》制定的；条例中界定了计算机软件的概念，明确了计算机软件著作权、计算机软件著作权的许可使用和转让等行为规范以及相应的法律责任。
- 《中华人民共和国著作权法实施条例》(2002 年 8 月 2 日中华人民共和国国务院令第 359 号)是根据《中华人民共和国著作权法》制定的；条例针对著作权法的具体实施过程做出规范。
- 《互联网上网服务营业场所管理条例》(2002 年 8 月 14 日国务院第 62 次常务会议通过，中华人民共和国国务院令第 363 号)是为了加强对互联网上网服务营业场所的管理，规范经营者的经营行为，维护公众和经营者的合法权益，保障互联网上网服务经营活动健康发展，促进社会主义精神文明建设制定的；条例中明确了互联网上网服务营业场所的设立、经营规范以及相应的罚则。
- 《信息网络传播保护条例》(2006 年 5 月 10 日国务院第 135 次常务会议通过，中华人民共和国国务院令第 468 号)是为保护著作权人、表演者、录音录像制作者的信息网络传播权，鼓励有益于社会主义精神文明、物质文明建设的作品的创作和传播，根据《中华人民共和国著作权法》制定的；条例中明确了权利人享有的信息网络传播权

有关行为的规范以及违规行为的刑事责任。

2.2.3 信息网络安全相关部门规范与其他规范

1. 国务院组成部门制定的规章和规范

国务院组成部门相当于内阁组成单位，是在国务院统一领导下，负责领导和管理某一方面的行政事务，行使特定的国家行政权力的行政机构，其设置由全国人民代表大会或其常务委员会决定。其涉及有关信息网络安全行政部门的规章规范包括：

（1）教育部制定发布的《高等学校知识产权保护管理规定》、《教育网站和网校暂行管理办法》、《高等学校信息公开办法》。

（2）科学技术部制定发布的《科学技术保密规定》。

（3）工业和信息化部制定发布的《计算机信息网络国际联网出入口信道管理办法》、《中国公用计算机互联网国际联网管理办法》、《计算机信息系统集成资质管理办法(试行)》、《互联网电子公告服务管理规定》、《公用电信间互联管理规定》、《电信经营许可证管理办法》、《信息系统工程监理暂行规定》、《中国互联网络域名管理办法》、《非经营性互联网信息服务备案管理办法》、《互联网 IP 地址备案管理办法》、《电子认证服务管理办法》、《互联网电子邮件服务管理办法》、《中国互联网络信息中心域名争议解决办法》、《互联网网络安全信息通报实施办法》、《木马和僵尸网络监测与处置机制》、《通信网络安全防护管理办法》、《规范互联网信息服务市场秩序若干规定》。

（4）公安部制定发布的《计算机信息系统安全专用产品检测和销售许可证管理办法》、《计算机信息网络国际联网安全保护管理办法》、《计算机病毒防治管理办法》、《联网单位安全员管理办法》、《互联网安全保护技术措施规定》、《信息安全等级保护管理办法》。

（5）商务部制定发布的《商业特许经营备案管理办法》。

（6）文化部制定发布的《互联网文化管理暂行规定》。

（7）人民银行制定发布的《个人信用信息基础数据库管理暂行办法》、《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》。

（8）审计署制定发布的《审计机关封存资料资产规定》。

2. 国务院直属特设机构制定的规章和规范

国有资产监督管理委员会，为国务院直属正部级特设机构。根据党中央决定，国有资产监督管理委员会成立党委，履行党中央规定的职责。国有资产监督管理委员会的监管范围是中央所属企业(不含金融类企业)的国有资产，具有独立的行政管理职能。其涉及有关信息网络安全行政部门的规章规范包括国有资产监督管理委员会制定发布的《中央企业商业秘密保护暂行规定》。

3. 国务院直属机构制定的规章和规范

国务院直属机构主管国务院的某项专门业务，具有独立的行政管理职能。其涉及有关

信息网络安全行政部门的规章规范包括如下：

（1）国家质量监督检验检疫总局制定发布的《信息安全产品测评认证管理办法》。

（2）国家广播电影电视总局制定发布的《互联网等信息网络传播视听节目管理办法》。

（3）国家新闻出版总署制定发布的《互联网出版管理暂行规定》、《互联网著作权行政保护办法》、《电子出版物出版管理规定》。

4. 国务院直属事业单位制定的规章和规范

国务院直属事业单位不是国家行政机关，但国务院授权其中一些单位行使一定的行政职能。其涉及有关信息网络安全行政部门的规章规范包括如下：

（1）中国银行业监督管理委员会制定发布的《电子银行安全评估指引》、《商业银行信息科技风险管理指引》。

（2）中国证券监督管理委员会制定发布的《证券经营机构营业部信息系统技术管理规范（试行）》、《期货交易所、期货经营机构信息技术管理规范（试行）》、《上市公司股东大会网络投票系统技术管理规范（试行）》、《证券期货业网络与信息安全信息通报暂行办法》、《证券期货业信息安全保障管理暂行办法》、《进入风险处置程序证券公司信息系统交接技术指引》、《证券投资基金销售业务信息管理平台管理规定》。

（3）国务院新闻办公室制定发布的《互联网站从事登载新闻业务管理暂行规定》、《互联网新闻信息服务管理规定》。

5. 国务院部委管理的国家局制定的规章和规范

国务院部委管理的国家局，现在除国家信访局由国务院办公厅管理外，都是国务院组成部门管理的国家行政机构，主管特定业务，行使行政管理职能。其涉及有关信息安全行政部门的规章规范包括如下：

（1）国家烟草专卖局制定发布的《烟草行业计算机信息网络安全保护规定》、《烟草行业计算机信息系统保密管理暂行规定》、《烟草行业信息系统技术管理规定（试行）》。

（2）国家食品药品监督管理局制定发布的《互联网药品信息服务管理办法》。

（3）国家保密局制定发布的《计算机信息系统保密管理暂行规定》、《涉及国家秘密的通信、办公自动化和计算机信息系统审批暂行办法》、《计算机信息系统国际联网保密管理规定》、《涉及国家秘密的计算机信息系统集成资质管理办法》。

（4）国家密码管理局制定发布的《商用密码科研管理规定》、《商用密码产品生产管理规定》、《商用密码产品销售管理规定》、《商用密码产品使用管理规定》、《境外组织和个人在华使用密码产品管理办法》、《电子认证服务密码管理办法》。

6. 最高人民法院、最高人民检察院关于相关法律问题的司法解释

最高人民法院是中华人民共和国最高审判机关，负责审理各类案件，制定司法解释，监督地方各级人民法院和专门人民法院的审判工作，并依照法律确定的职责范围，管理全国法院的司法行政工作。

最高人民检察院是中华人民共和国最高检察机关，是法律监督机关，主要任务是领导地

方各级人民检察院和专门人民检察院依法履行法律监督职能，保证国家法律的统一和正确实施。

由最高人民法院、最高人民检察院负责提出有关法律问题的司法解释，其中涉及有关信息网络安全内容相关的司法解释包括：

- 《最高人民法院关于审理扰乱电信市场管理秩序案件具体应用法律若干问题的解释》。
- 《最高人民法院关于审理涉及计算机网络著作权纠纷案件适用法律若干问题的解释》。
- 《最高人民法院关于审理为境外窃取、刺探、收买、非法提供国家秘密、情报案件具体应用法律若干问题的解释》。
- 《最高人民法院关于审理涉及计算机网络域名民事纠纷案件适用法律若干问题的解释》。
- 《最高人民法院关于审理涉及计算机网络著作权纠纷案件适用法律若干问题的解释》。
- 《最高人民法院、最高人民检察院关于办理利用互联网、移动通信终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释》。
- 《最高人民法院、最高人民检察院关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释》。
- 《最高人民法院、最高人民检察院关于办理赌博刑事案件具体应用法律若干问题的解释》。
- 《最高人民法院关于修改《最高人民法院关于审理涉及计算机网络著作权纠纷案件适用法律若干问题的解释》的决定(二)》。
- 《最高人民法院、最高人民检察院关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释(二)》。
- 《最高人民法院关于审理危害军事通信刑事案件具体应用法律若干问题的解释》。
- 《最高人民法院关于审理破坏电力设备刑事案件具体应用法律若干问题的解释》。
- 《最高人民法院、最高人民检察院关于办理妨害信用卡管理刑事案件具体应用法律若干问题的解释》。
- 《最高人民法院、最高人民检察院关于办理利用互联网、移动通信终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释(二)》。
- 《最高人民法院关于审理破坏广播电视设施等刑事案件具体应用法律若干问题的解释》。
- 《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》。

7. 其他规范

各省、自治区、直辖市等地方政府也依据各地方的实际情况制定发布了一些地方性法规来规范相关信息网络安全领域的行为。

习　　题

1. 我国信息网络安全法律法规体系构成有哪些?
2. 简述我国信息网络安全法律法规的作用。

第 3 章

网络安全监督管理

【内容提要】

本章主要介绍信息网络安全监督管理工作的相关内容，包括互联网单位备案管理、互联网运营单位管理、互联网信息服务单位管理、联网单位管理、计算机病毒等破坏性程序防治管理等。通过学习，掌握信息网络安全监督管理工作的工作内容、工作方法、工作要求及行政处罚等方面的规定。

3.1 网络安全监督管理概述

网络安全监督管理工作，是指公安机关依照国家法律和法规，运用行政手段，对信息网络安全进行监督、检查和指导，有效预防信息网络违法犯罪，依法查处信息网络领域违法行为，维护网上公共秩序，保障社会生活正常运行的行政管理工作。信息网络安全监督管理工作是公共信息网络安全监察工作的重要内容，是国家行政管理的组成部分。

信息网络安全监督管理是由公安机关网络安全保卫部门依法公开实施的行政管理行为。《中华人民共和国人民警察法》第 6 条第 12 款规定，“公安机关的人民警察按照职责分工，依法履行监督管理计算机信息系统的安全保卫工作的职责”。公安机关网络安全保卫部门通过开展信息网络安全监督管理工作，达到维护信息网络安全的目的。

网络安全监督管理工作的对象包括互联网运营单位、互联网信息服务单位、联网单位、互联网上网服务营业场所和重要信息系统。本章重点介绍互联网运营单位、互联网信息服务单位和联网单位的监督管理工作。

3.1.1 网络安全监督管理指导思想

以维护信息网络领域安全为主要任务，依托基层基础工作，实行监督管理与技术防控相结合，依法管理、依法行政，增强网上防范控制能力，建立现代化的管理方式和长效机制，为开展网上工作、维护网络秩序、打击涉网犯罪提供重要保障。

1. 打牢基础，协调发展

信息网络安全监督管理工作是国家赋予公安机关的一项重要法定职责，是公安机关开展网上工作的重要支撑和重要基础。只有高度重视并扎实做好监督管理工作，与其他网络

安全保卫工作协调发展，齐头并进，才能为公安机关开展网上工作构建起坚实的基础支撑。

2. 群防群治，综合治理

信息网络安全监督管理工作是一项社会化综合治理工程，是全社会共同的责任，必须坚持“谁主管谁负责，谁经营谁负责，谁受益谁负责”的原则，充分调动网络运营单位、信息服务单位、联网单位和广大网民的积极性、主动性，构建全社会共同参与、群防群治的信息网络安全监督管理工作新格局，实现对信息网络安全的综合治理。

3. 积极防御，综合防范

加强对互联网安全的监督管理，落实各项安全保护管理制度和安全保护技术措施，有效遏制境内外敌对势力、敌对分子和一些别有用心的人利用境内网上各种信息传播渠道对我进行煽动、渗透和破坏活动，加强对计算机病毒和网络攻击等网络安全威胁事件的预警发现和快速处置能力，积极推进信息系统安全等级保护，确保基础信息网络和重要信息系统的安全运行。

4. 紧跟发展，掌握主动

互联网信息产业发展迅速，各种新兴业务层出不穷，公安机关网络安全保卫部门要密切关注互联网发展，对信息网络安全监督管理工作面临的形势、任务和挑战有清醒认识，对各种新兴的网络应用和服务主动介入，适时开展调查研究，坚持“正确引导、趋利避害、为我所用”的原则，加强对网络服务提供商的监督管理，明确责任、落实义务，做好各项管理制度和安全技术防范措施，牢牢把握网上控制的主动权。

5. 严格执法，热情服务

公安机关网络安全保卫部门必须依照有关法律法规的规定，及时、主动上门指导网络运营单位、联网单位落实安全保护管理制度和技术措施，做好网络安全知识宣传，建立方便、快捷的办事渠道，以热情的服务树立网络警察的形象。对“重建设，轻安全；重应用，轻管理”的单位，要采取必要的行政管理手段、法律手段强制其落实各项制度措施。

3.1.2　网络安全监督管理工作特点

信息网络安全监督管理具有不同于国家其他社会组织活动工作的特点，具体表现如下。

1. 管理对象的广泛性

(1) 互联网运营单位：包括互联网接入服务单位(Internet Service Provider，简称 ISP)、互联网数据中心(Internet Data Center，简称 IDC)等。

(2) 互联网信息服务单位(Internet Content Provider，简称 ICP)：包括网站、聊天室、论坛、搜索引擎、电子邮件、互联网娱乐平台、点对点服务、短信息、电子商务、网上视音频、声讯信息等服务单位。

(3) 联网单位。

(4) 互联网上网服务营业场所。

(5) 重要信息系统：涉及电力、民航、铁路等国家重要基础设施，也涉及金融、证券、保

险、工商、税务、海关等重点单位和重要政府部门的内部应用网络系统。

2. 管理方式的复杂多样性

管理对象的广泛性，决定了具体管理方式的多样性。尤其多个对象在现实中往往交织在一起，致使信息网络安全监督管理工作变得更加复杂。既有行政管理的一般管理方法，如指导、检查、督促和查处等，也有公安机关网络安全保卫部门所特有的特殊管理方式。另外，互联网新型服务以及新的管理对象层出不穷，也带来了新的管理方式。

3. 管理措施的强制性

监督管理工作不同于一般意义上的行政管理工作，它是以国家赋予公安机关治安强制措施作为后盾。

4. 管理活动的社会性

监督管理工作既是国家事务，也是一项社会事业。一方面，信息网络安全监督管理工作主要是面向社会公开进行的，关系到国家、集体和群众方方面面具体的利益；另一方面，信息网络安全监督管理工作的组织开展也离不开社会力量，依靠人民群众参与信息网络安全管理活动，也是维护社会治安秩序的客观需要。

3.1.3 网络安全监督管理主要任务

信息网络安全监督管理工作既包括公安机关网络安全保卫部门依法对互联网单位的监督、检查、管理工作，也包括公安机关网络安全保卫部门依法对重要信息系统的监督、指导工作。其主要任务大体分为以下几个方面。

1. 互联网安全管理

(1) 指导督促互联网单位的备案工作。

(2) 监督、检查互联网单位落实安全管理制度和安全保护技术措施。

(3) 监督管理互联网上网服务营业场所，严格进行安全审核和日常检查。

2. 监督、检查、指导重要信息系统的信息安全等级保护工作

3. 处置网上有害信息

4. 查处信息网络违法违规行为

5. 组织开展计算机病毒等破坏性程序的日常防治管理

6. 组织开展重大活动的信息安全保卫工作

7. 组织计算机安全员培训

3.1.4 网络安全监督管理主要方法

1. 开展基础调查

基础调查是公安机关网络安全保卫部门一项经常性和基础性的工作，是了解和掌握信息网络运营、服务和使用单位基本情况的重要手段，是总结经验教训、改进管理方式、提高管理水平的重要方法。

（1）建立畅通的交流和信息传输渠道。在公安机关和被管理的互联网单位之间建立纵向的信息交流和传输渠道，实行案事件报告制度、情况数据定期上报和数据变更及时上报等制度，全面掌握本地 ISP、IDC、ICP、联网单位的基本情况，熟悉网络的拓扑结构；在公安机关内部建立横向的交流渠道，实行情况通报制度，共享信息和数据。

（2）开展基础调查。按照特定时期的工作需要，组织开展基础调查专项工作，针对某一方面基础数据、基本情况进行调查和普查。

（3）对基础数据进行统计、分析。对大量数据进行统计、关联性分析研究，从中发现翔实的、有用的、规律性的基础数据，为制定管理计划和措施提供资料。

（4）建立基础数据库。通过基础调查获得的数据和掌握的情况都应建库管理，长期积累，及时更新；还要建立数据资料采集、录入的工作规范。

2. 建立信息网络安全监督管理制度

依照国家有关法律法规，结合安全管理工作实际，制定、完善和落实一整套针对性强，责、权明确的安全管理规章和制度，对重要信息系统单位、重点要害部位、上网服务场所、互联网联网单位、安全产品进行规范化管理。

3. 落实互联网安全保护技术措施

按照《互联网安全保护技术措施规定》的要求，监督管理互联网服务提供者、联网使用单位落实互联网安全保护技术措施。采取的互联网安全保护技术措施应当具有符合公共安全行业技术标准的联网接口，并保障互联网安全保护技术措施功能的正常发挥。

4. 建设社会支撑力量

“专群结合、依靠群众”是确保信息网络安全监督管理工作顺利进行的重要保障，通过发动、组织社会力量参与信息网络安全防范和管理工作，可以有效弥补公安机关警力不足，将违法犯罪行为置于群众和社会的监督之下。

（1）建立日常联络机制。

（2）安全组织和安全员的建设和管理。

（3）建立、健全网上信息安全的协管队伍。

（4）组织开展行业自律。

5. 加强宣传教育

（1）加强日常网络安全知识宣传。通过互联网站、本地主流新闻媒体，或者通过印制宣传书籍、画册的形式开展互联网日常安全的教育宣传活动，向社会宣传国家法律法规，指导开展信息网络安全防范；专项行动期间还应配合工作需要进行专题的宣传教育。

（2）通过计算机安全员培训进行集中宣传教育。

（3）管理工作中的宣传教育。网络安全保卫部门在日常管理执法工作中，有针对性地宣传法律法规，督促落实制度和技术措施，提高被管理单位和个人的安全意识；依法对违法违规行为进行处罚，起到惩戒教育的作用。

3.2 互联网单位管理

3.2.1 备案管理

备案是互联网安全管理的基础。备案制度的实施,可以增强连接互联网的单位的安全管理意识,建立健全安全管理制度,督促其依法履行社会责任;而备案工作也是公安机关网络安全保卫部门依法开展的警务工作,可以有效防止和控制危害我国国家利益的有害信息流入和涉及我国国家机密的重要信息流出。

1. 备案法律依据

1)《中华人民共和国计算机信息系统安全保护条例》(国务院147号令)

第十一条规定:"进行国际联网的计算机信息系统,由计算机信息系统的使用单位报省级以上人民政府公安机关备案"。

2)《计算机信息网络国际联网安全保护管理办法》(公安部第33号令)

第十一条　用户在接入单位办理入网手续时,应当填写用户备案表。备案表由公安部监制。

第十二条　互联单位、接入单位、使用计算机信息网络国际联网的法人和其他组织(包括跨省、自治区、直辖市联网的单位和所属的分支机构),应当自网络正式联通之日起三十日内,到所在地的省、自治区、直辖市人民政府公安机关指定的受理机关办理备案手续。

前款所列单位应当负责将接入本网络的接入单位和用户情况报当地公安机关备案,并及时报告本网络中接入单位和用户的变更情况。

第十四条　涉及国家事务、经济建设、国防建设、尖端科学技术等重要领域的单位办理备案手续时,应当出具其行政主管部门的审批证明。

前款所列单位的计算机信息网络与国际联网,应当采取相应的安全保护措施。

第十六条　公安机关计算机管理监察机构应当掌握互联单位、接入单位和用户的备案情况,建立备案档案,进行备案统计,并按照国家有关规定逐级上报。

3)《公安部关于对与国际联网的计算机信息系统进行备案工作的通知》

与国际联网的计算机信息系统的使用单位和个人,应当在网络正式联通后的三十日内,到所在地的省、自治区、直辖市人民政府公安机关指定的地(市)级或者县(市)级人民政府公安机关办理备案手续。

已经与国际联网的计算机信息系统,其使用单位和个人应当在本通知公布之日起三十日内,到所在地(市)级或者县(市)级人民政府公安机关补办备案手续。

与国际联网的计算机信息系统的使用单位和个人的联网方式变更或者终止联网时,应当在三十日内通知所在地(市)级或者县(市)级人民政府公安机关。

2. 备案对象和要求

凡中华人民共和国境内的互联网运营单位(包括ISP、IDC)、互联网信息服务单位

(ICP)、联网单位、互联网上网服务营业场所和个人联网用户均为备案对象。

注意：以上单位凡服务器托管地与维护地不在同一行政区划内的，必须同时向服务器托管地和维护地的公安机关网络安全保卫部门申请备案。

各互联网单位备案具体要求如下：

1）互联网接入服务单位

互联网接入服务单位(Internet Service Provider，ISP)是指提供互联网接入网络运行的单位。接入网络是指通过接入互联网络进行国际联网的计算机信息网络，接入网络可以是多级连接的网络。

互联网接入服务单位办理备案需提供的资料清单如下：

(1) 中华人民共和国公安部网络安全保卫局印发的备案表一式两份(加盖备案单位公章)。

(2) 本单位的计算机信息网络安全组织成员名单，包括单位负责人、两名计算机安全员，含联系方式。

(3) 计算机安全员证书复印件。

(4) 本单位的计算机信息网络安全保护管理制度，包括互联网公用账号登记制度、互联网安全保护管理制度、互联网安全应急处置制度等。

(5) 安全保护技术措施。包括：网络安全审计、防病毒、防黑客攻击措施等。

(6) 本单位的网络拓扑图(标明内部 IP 使用情况)。

(7) 本单位的 IP 分配、使用和变更情况。

(8) 本单位的接入方式使用、新增和变更情况。

(9) 本单位的用户注册登记、使用与变更情况(包括固定 IP 用户、动态 IP 用户、托管主机用户)。

(10) 在提交上述材料的基础上，还需按照其他法律法规要求提交相关管理部门颁发的证照的复印件，如工商部门核发的营业执照副本复印件，信息产业部及各省市通信管理部门颁发的相关经营许可证等。

注意：公安机关网络安全保卫部门在受理互联网接入服务单位备案的同时，还要督促互联网接入服务单位报送接入本网络的联网用户(包括单位和个人)的情况，并及时以电子表格的形式报告本网络中接入用户的变更情况，包括用户姓名、联系电话、地址、身份证复印件、开户账号等。

除未开设个人网站、网页的个人联网用户属于上述情况之外，其他 IDC、ICP 等互联网接入服务单位的联网用户需直接到公安机关网络安全保卫部门备案。

2）互联网数据中心

互联网数据中心(Internet Data Center，IDC)是指向企业、商户或网站服务器群提供大规范、高质量、安全可靠的专业化服务托管、虚拟空间租用、网络带宽出租等服务的单位。

互联网数据中心办理备案需提供的资料清单如下：

(1) 中华人民共和国公安部网络安全保卫局印发的备案表一式两份(加盖备案单位公章)。

(2) 本单位的计算机信息网络安全组织成员名单，包括本单位负责人、两名计算机安全员，含联系方式。

(3) 计算机安全员证书复印件。

(4) 本单位的计算机信息网络安全保护管理制度。包括信息发布审核制度、24 小时交互栏目信息巡查制度、互联网公用账号登记制度、互联网安全管理制度、互联网安全应急处置制度等。

(5) 安全保护技术措施。包括交互式栏目必须有关键字过滤技术措施、网络安全审计、防病毒防黑客攻击等措施。

(6) 本单位的网络拓扑图(标明内部 IP 使用情况)。

(7) 本单位 IP 分配、使用和变更情况。

(8) 本单位所有托管主机服务用户的基本情况，包括网站相关资料、负责人信息、联系方式等。

(9) 在提交上述材料的基础上，还需按照其他法律法规要求提交相关管理部门颁发的证照的复印件。

注意：公安机关网络安全保卫部门在受理互联网数据中心备案的同时，还要督促互联网数据中心报送本单位虚拟空间服务用户的情况，并及时以电子表格的形式报告虚拟空间服务用户的变更情况，包括用户虚拟空间的服务器地址、用户网站信息，用户姓名、联系电话、地址等。

3) 互联网信息服务单位

互联网信息服务单位(Internet Content Provider，ICP)是指以互联网为载体，提供信息发布和信息查询服务的单位或个人，包括各类网站、个人主页和提供短信内容服务、游戏服务、邮件服务以及其他互联信息服务的单位或个人。

互联网信息服务分为经营性 ICP 和非经营性 ICP。

互联网信息服务单位办理备案需提供的资料清单如下：

(1) 中华人民共和国公安部网络安全保卫局印发的备案表一式两份(加盖备案单位公章)。

(2) 本单位的计算机信息网络安全组织成员名单，包括本单位负责人、两名计算机安全员，含联系方式；个人网站应提交计算机安全员名单及联系方式。

(3) 计算机安全员证书复印件。

(4) 本单位的计算机信息网络安全保护管理制度。包括：信息发布审核制度、24 小时交互栏目信息巡查制度、互联网公用账号登记制度、互联网安全管理制度、互联网安全应急处置制度等。

(5) 安全保护技术措施。包括：交互式栏目必须有关键字过滤技术措施、网络安全审计、防病毒防黑客攻击等措施。

(6) 本单位的网络拓扑图(标明内部 IP 使用情况)。

(7) 网站网页基本情况，网页栏目设置与变更及栏目负责人情况。

(8) 提供服务或开办栏目的种类，重点说明新闻、交互式栏目、邮件服务、搜索引擎等情况；针对各种服务类型制定的安全保护管理制度及安全保护技术措施等。

(9) 虚拟主机用户情况。

(10) 在提交上述材料的基础上，还需按照其他法律法规要求提交工商部门核发的营业执照副本复印件；经营性网站必须提供通信管理部门核发的电信与信息服务业务经营许可证，非经营性网站必须提交通信管理部门核发的备案证书；从事新闻、出版、教育、医疗保健、药品和医疗器械等互联网信息服务的单位，还需提交审核证明等相关管理部门颁发的证照复印件。

注意：公安机关网络安全保卫部门在受理互联网信息服务单位备案的同时，还要督促互联网信息服务单位报送本单位提供出租网站服务用户的情况，并及时以电子表格的形式报告出租网站服务用户的变更情况，包括用户服务器的地址，所有者姓名、联系电话、详细地址、服务内容等。

同时具备 ISP、IDC、ICP 三种业务功能中两种或两种以上的，或者在原有业务功能基础上增加新业务功能的互联网单位，必须就每一种业务功能到公安机关网络安全保卫部门依法履行备案义务。具体要求：具备两种或两种以上业务功能的，必须一次性提交相关业务功能备案材料(参照 ISP、IDC 和 ICP 备案需提交的材料)，到公安机关进行综合备案；在原有业务功能基础上增加新业务功能的，必须提交新业务功能对应的备案材料，到公安机关进行变更备案。

4) 互联网联网单位

互联网联网是指中华人民共和国境内的计算机互联网络、专业计算机信息网络、企业计算机信息网络，以及其他通过专线进行国际联网的计算机信息网络同外国的计算机信息网络相连接。互联网联网单位是指通过接入网络与互联网连接的计算机信息网络用户，包括单位用户及个人用户。社区、学校、图书馆、宾馆、咖啡馆、娱乐休闲中心等向特定对象提供上网服务的场所也纳入互联网联网单位管理。

互联网联网单位办理备案需提供的资料清单如下：

(1) 中华人民共和国公安部网络安全保卫局印发的备案表一式两份(加盖备案单位公章)。

(2) 本单位的计算机信息网络安全组织成员名单，包括单位负责人、两名计算机安全员，含联系方式。

(3) 计算机安全员证书复印件。

(4) 本单位的计算机信息网络安全保护管理制度，包括互联网安全保护管理制度、互联网安全应急处置制度等。

(5) 安全保护技术措施。包括：网络安全审计、防病毒、防黑客攻击措施等。

(6) 本单位的网络拓扑图(标明内部 IP 使用情况)。

(7) 在提交上述材料的基础上，还需提供工商行政管理部门核发的营业执照副本复印件。

5) 互联网上网服务营业场所

互联网上网服务营业场所是指通过计算机等设备向公众提供互联网上网服务的网吧、

电脑休闲室等营业性场所。

互联网上网服务营业场所办理备案需提供的资料清单如下：

(1) 中华人民共和国公安部网络安全保卫局印发的备案表一式两份(加盖备案单位公章)。

(2) 本单位的计算机信息网络安全组织成员名单，包括单位负责人、两名计算机安全员，含联系方式。

(3) 计算机安全员证书复印件。

(4) 本单位的计算机信息网络安全保护管理制度。包括互联网安全保护管理制度、互联网安全应急处置制度等。

(5) 互联网上网服务营业场所安全保护管理制度，包括上网人员登记制度，对上网人员可能利用互联网络从事违法犯罪活动进行巡查、举报、制止制度等。

(6) 互联网安全保护技术措施。包括网络安全审计、防病毒、防黑客攻击措施等。

(7) 互联网上网服务营业场所技术支持单位信息，包括单位名称、地址、主要联系人、联系方式、技术支持类型等。

(8) 本单位的安全管理软件安装使用情况，包括管理软件名称、型号、销售许可证号、生产厂家、联系人等。

(9) 本单位的网络拓扑图(标明内部 IP 使用情况)。

(10) 本单位的场地结构图(标明计算机位置编号与 IP 地址对应情况)。

(11) 本单位营业场所方位图。

(12) 租房协议(房屋是自己的需提交房产证复印件)。

(13) 在提交上述材料的基础上，还需按照其他法律法规要求提交工商部门核发的营业执照，文化部门核发的网络经营许可证，消防部门核发的消防安全审核意见书等相关管理部门颁发的证照的复印件。

6) 个人联网用户

个人联网用户是指以个人使用为目的，接入互联网的用户。

个人联网用户备案须知：

(1) 个人联网用户备案工作由互联网接入服务单位协助公安机关进行。

(2) 个人联网用户备案由互联网接入服务单位负责实名登记。个人用户在开通互联网时要提供相关基本资料，包括：个人用户姓名、联系电话、地址、身份证复印件、开户电话、开户账号、IP 用途等。资料先保存在接入服务单位，由接入服务单位汇总、整理后，统一报给公安机关备案。原则上，一般个人用户不直接到公安机关办理备案手续(个人用户计划开办网站、网页等互联网信息服务的，应当在接入服务商处登记相关资料时予以说明，并在网站开办后按网站、网页备案程序进行备案)。

(3) 互联网接入服务单位按照规定时间，将个人用户备案资料汇总、整理后，按照统一数据格式，以电子数据报表形式报送公安机关网络安全保卫部门。

(4) 公安机关网络安全保卫部门指导互联网接入服务单位调整、完善个人用户备案电

子数据报表数据项。

3. 备案管辖

(1) 各地级以上(含地级)人民政府公安机关网络安全保卫部门对物理位置在本行政区划内与互联网相连接的计算机信息系统(服务器)或维护人员都具有备案管辖权。

(2) 各地级以上(含地级)人民政府公安机关网络安全保卫部门对分别落于不同地级市的与互联网相连接的计算机信息系统(服务器)所在单位或维护人员、维护权在本地的都具有备案管辖权,即共同管辖。

备案管辖以计算机信息系统服务器所在地的公安机关网络安全保卫部门为主,负有监督管理责任,必须加强管理,及时指导、督促其履行备案义务。

(3) 计算机信息系统服务器所在地的公安机关网络安全保卫部门有义务将互联网单位的有关资料在备案结束后 15 天内抄送给计算机信息系统所在单位或维护人员、维护权所在地的公安机关网络安全保卫部门。

抄送互联网单位资料的主要内容包括:互联网单位和个人的基本资料、服务器资料、网站和网上服务相关资料、维护人员基本情况等。

(4) 与互联网相连接的互联网信息系统(服务器)或维护人员所在单位或个人都必须向服务器托管地和维护地的公安机关网络安全保卫部门申请备案。

4. 备案程序

1) 互联网单位备案程序

(1) 互联网单位下载或到公安机关网络安全保卫部门领取备案相关资料与表格。

(2) 各互联网单位按照要求填写备案表,由单位领导签字盖章,在其网络正式联通之日起 30 日内与其他需提交的材料一起提交到公安机关网络安全保卫部门。

(3) 公安机关网络安全保卫部门对各互联网单位提交的备案资料进行初审(对备案材料的真实性和合法性进行审核)和复审(按照备案表填写的内容逐项实地核查),审核无误后加盖公章,统一编号建立备案档案。审核中若发现各项制度未按要求落实或提交材料不齐的,退回材料,限期整改,符合要求后,可申请再次审核。

(4) 各互联网备案单位要记录好反馈的受理编号及密码,凭受理编号及密码可以登录修改备案资料、查看审核结果。审核通过后,各互联网备案单位要领取备案回执、备案证书,下载网站的备案图标。

(5) 如果是网站备案,除了下载备案图标、报警岗亭图标和“警警察察”图标外,还要及时将备案图标、报警岗亭图标置于网站首页的下方,“警警察察”图标置于交互式栏目入口处,并按要求完成相应的链接。

2) 公安机关网络安全保卫部门受理备案材料工作流程

公安机关网络安全保卫部门受理备案材料工作流程如图 3-1 所示。

3) 公安机关网络安全保卫部门核实检查备案工作流程

公安机关网络安全保卫部门核实检查备案工作流程如图 3-2 所示。

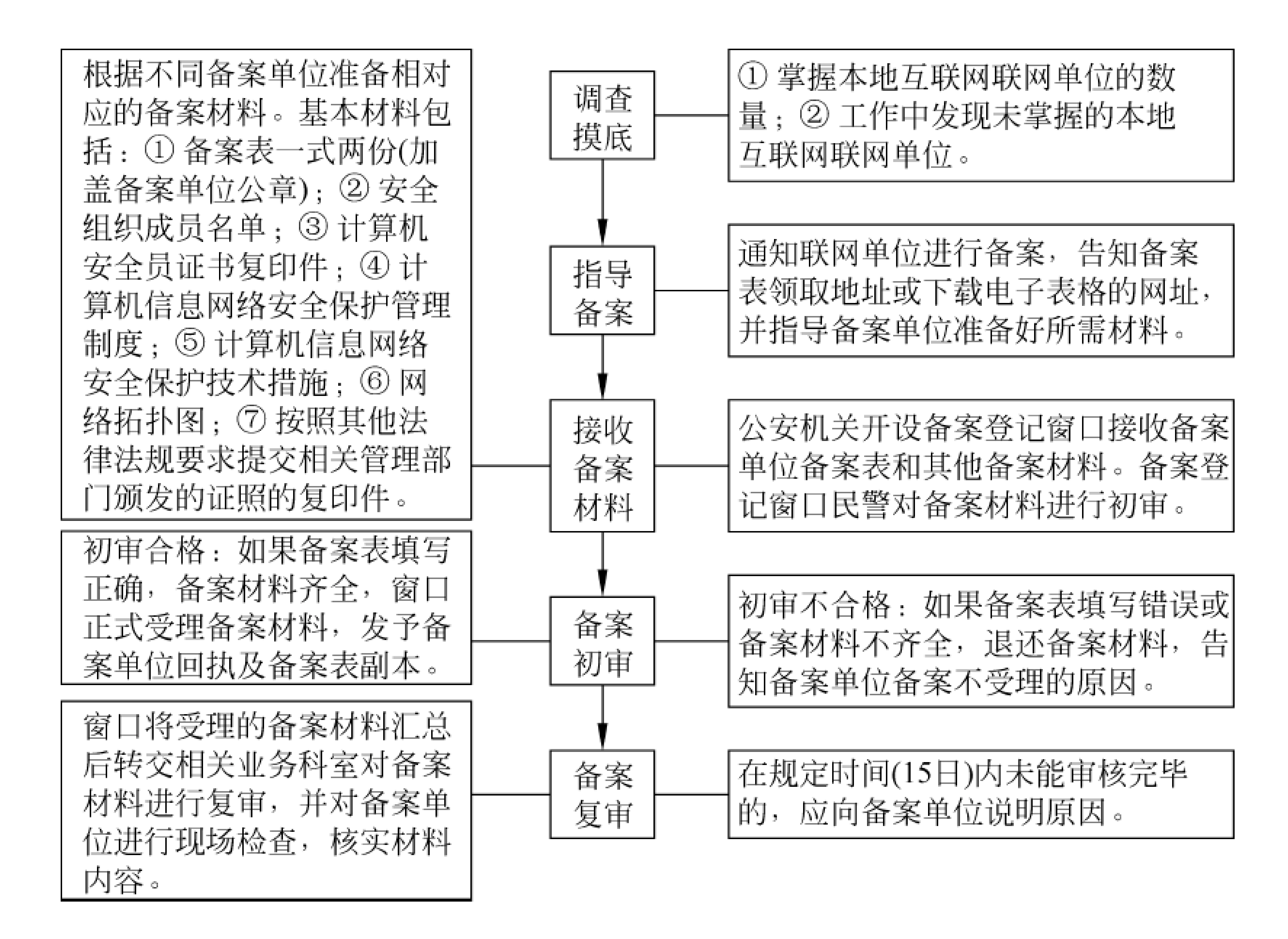


图 3-1 备案材料受理工作流程

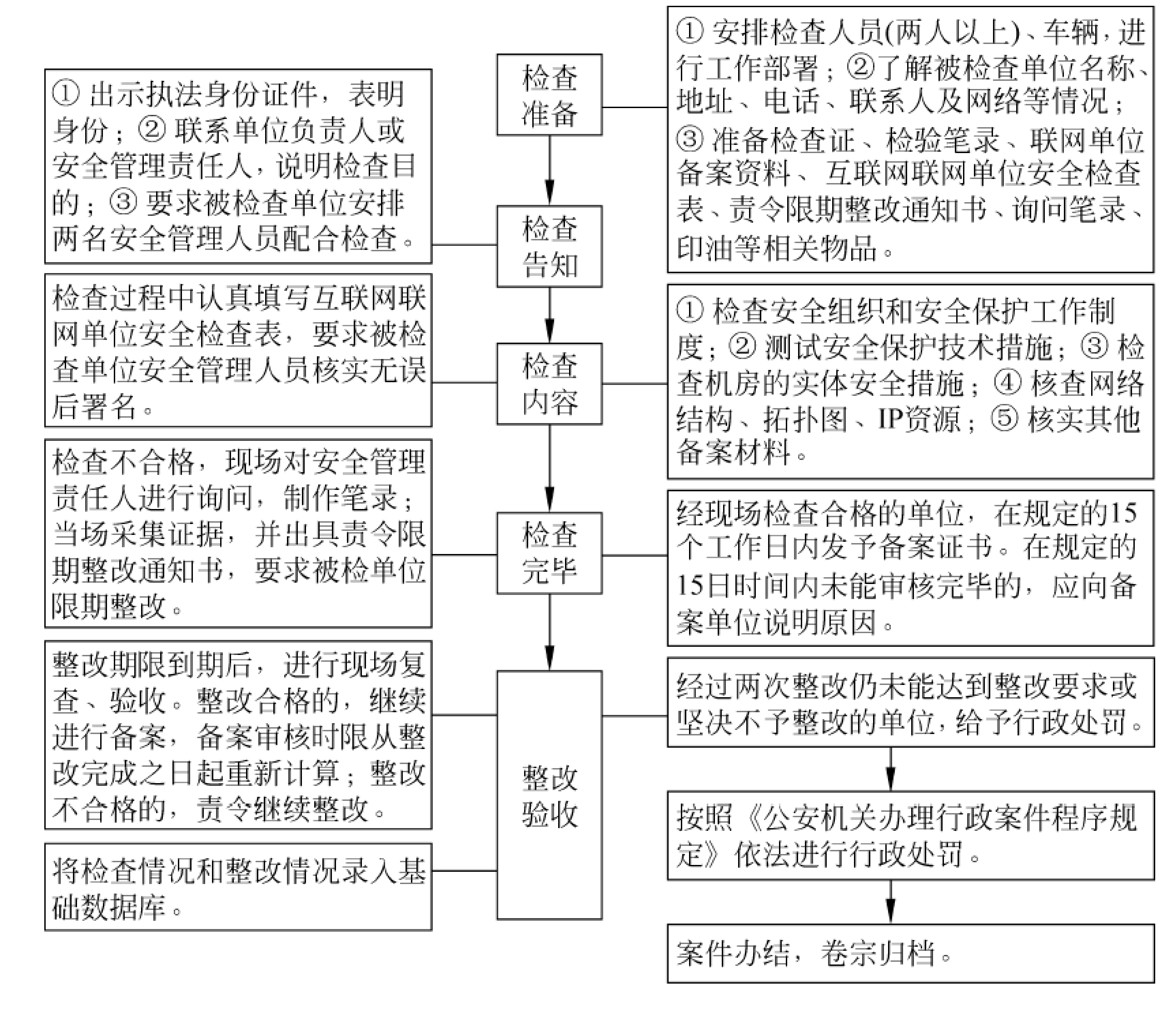


图 3-2 备案核实检查工作流程

5. 备案罚则

对不按规定履行备案义务的单位或个人，不落实安全管理制度和措施的，按照《中华人民共和国计算机信息系统安全保护条例》第二十条和《计算机信息网络国际联网安全保护管理办法》第二十三条规定，由公安机关责令限期改正，给予警告，有违法所得的，没收违法所得；在规定的限期内未改正的，对单位的主管负责人员和其他直接责任人员可以并处五千元以下的罚款，对单位可以并处一万五千元以下的罚款；情节严重的，并可以给予六个月以内的停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格。

6. 相关表格

计算机信息网络国际联网单位备案表

填表时间：年　月　日　　　　　　　　　　　　　　　　　　　　　　编号：

<table>
<tr><td>单位名称</td><td colspan="2"></td><td colspan="2">单位负责人
（法人代表）</td><td colspan="2"></td></tr>
<tr><td>通信地址</td><td colspan="6"></td></tr>
<tr><td>邮政编码</td><td colspan="2"></td><td colspan="2">联系电话</td><td colspan="2"></td></tr>
<tr><td rowspan="3">备案单位
安全管理员</td><td>姓名</td><td></td><td>电话</td><td></td><td>传真</td><td></td></tr>
<tr><td>姓名</td><td></td><td>电话</td><td></td><td>传真</td><td></td></tr>
<tr><td colspan="2">E-mail 地址</td><td colspan="4"></td></tr>
<tr><td>网络名称</td><td colspan="3"></td><td colspan="2">域名注册服务商</td><td></td></tr>
<tr><td>接入网络服务商</td><td colspan="3"></td><td colspan="2">申请入网时间</td><td></td></tr>
<tr><td>所属网络</td><td colspan="6">○中国电信　○中国教育和科研计算机网　○中国网通
○中国联通　○中国铁通　○中国移动　○其他网络</td></tr>
<tr><td>服务种类</td><td colspan="6">□接入服务　□ 虚拟空间租用　□ 主机托管　□ 电子邮件服务
□个人主页　□ 论坛、留言板、BBS 服务　□ FTP 服务
□WWW 服务　□ 聊天室　□ 电子商务　□ 即时通信服务
□短信息服务　□ 宽带多媒体服务　□ 网络游戏　□ 其他</td></tr>
<tr><td>服务性质</td><td colspan="6">○ ISP　○ ICP　○ IDC　○互联网单位用户　○ 其他</td></tr>
<tr><td>安全措施</td><td colspan="6">□ 防病毒　□ 防入侵　□ 信息过滤　□ 人工巡查　□ 其他</td></tr>
<tr><td>审计方式</td><td colspan="6">□ 人工登记　□ 系统日志　□ 专用审计软件　□ 其他</td></tr>
<tr><td>网络概况</td><td colspan="6">下级网络（详情填附表）________个，联网主机________台</td></tr>
<tr><td>网站、网页类型</td><td colspan="6">□ 自管主机　□ 托管主机　□ 虚拟空间　□ 虚拟主机</td></tr>
<tr><td>联网单位
接入方式</td><td colspan="6">□ DDN 专线　□ 光纤　□ 城域 IP 网　□ ADSL　□ ISDN
□ 拨号　□ Cable Modem　□ 其他</td></tr>
<tr><td>IP 地址范围</td><td colspan="6"></td></tr>
<tr><td>出口路由器 IP</td><td colspan="6"></td></tr>
<tr><td>域名服务器 IP</td><td colspan="6"></td></tr>
<tr><td>邮件服务器 IP</td><td colspan="6"></td></tr>
<tr><td colspan="3">备案单位盖章

年　月　日</td><td colspan="4">公安机关盖章

年　月　日</td></tr>
</table>

附表一　下级网络、虚拟空间租用及主机托管服务备案表

编号：

类型	○下级网络　○虚拟空间租用　○主机托管		
网络名称			
单位名称			
所在省(区市)		所在地(市)	
联系人		联系电话	
通信地址			
域名			
IP 地址段			

附表二　固定 IP 地址个人用户入网备案表(ISP 提供)

编号：

姓名		性别		出生日期	
证件种类		证件编号			
职业类别	○国家公务员　○企事业单位人员　○军人 ○农民　○商业、服务业人员　○学生、教师 ○无业人员　○其他				
联系电话					
上网地址					
通信地址					
IP 地址					
申请入网时间					
IP 地址分配单位					

***** 计算机国际联网单位备案审批表**

填表时间：年　月　日　　　　编号：

备案单位	
网站域名	
所提交备案材料清单	❑1．公共信息网络安全保卫部门统一印制的备案表一式两份(加盖公章)； ❑2．经营性互联网站需提交通信管理部门核发的《电信与信息服务业务经营许可证》、工商部门核发的《营业执照》副本复印件； ❑非经营性网站需提交建立网站用途及栏目说明性文件(加盖单位公章)； ❑个人网站需提交有效身份资料证照复印件； ❑3．单位计算机信息网络安全组织成员名单(包括本单位主管领导、两名计算机安全员，含联系方式)； ❑4．计算机安全员证书复印件； ❑5．单位计算机信息网络安全管理制度(包括：信息发布审核制度、24 小时交互式栏目信息巡查制度、互联网安全应急处置制度等)；

续表

备案单位			
网站域名			
所提交备案材料清单	❑6. 互联网信息网络安全技术措施解决方案(包括：交互式栏目必须有关键字过滤技术措施、日志审计、防病毒防黑客攻击措施等)； ❑7. 从事刊载新闻的网站还必须提交新闻管理部门的批准文件； ❑8. 提供虚拟主机服务的信息服务单位，除提交以上材料外，还必须提交使用本单位虚拟主机服务的所有用户的基本情况，包括 URL、负责人、联系方式； ❑9. 系统维护权落于外地，服务器托管于云南的网站，除提交以上材料外，还必须提交其系统维护权所在地主管公安机关出具的备案证明。		
受理人		受理时间	
备案编号录入			
审核民警意见			
领导审批意见			
档案接收情况		接收时间	
备注			

网站备案信息真实性核验单

网站主办者基本信息：(网站主办者填写)			
网站主办者名称		网站类型	□单位　□个人
网站域名			
网站备案信息核验内容：(接入服务单位填写)			
一、主体信息核验内容：			
核验网站主办者、网站负责人证件资质(网站类型为“个人”时只需核验个人证件资质，请在核验的对应证件下打“√”)			
单位证件资质：□组织机构代码证书　□工商营业执照　□事业法人证书　□社团法人证书　□军队代号　□其他			
个人证件资质：□身份证　□户口簿　□军官证　□港澳台胞证　□护照　□其他			
网站主办者、网站负责人证件号码报备信息是否正确　□是　□否			
是否留存网站主办者、网站负责人证件复印件　□是　□否			
是否当面采集并留存网站负责人照片　□是　□否			
二、联系方式核验内容：			
网站负责人手机号码报备信息是否正确　□是　□否			
网站负责人座机号码报备信息是否正确(网站类型为“个人”时选填)　□是　□否			
网站负责人电子邮箱报备信息是否正确　□是　□否			
网站负责人通信地址报备信息是否正确　□是　□否			
三、网站信息核验内容：			
网站名称报备信息是否规范　□是　□否		域名报备信息是否正确　□是　□否	

续表

网站服务内容/项目报备信息是否正确 □是 □否
是否有前置审批或专项审批文件(如有前置审批或专项审批文件,请在核验文件内容的对应类别下打“√”) □是 □否
□新闻 □出版 □教育 □医疗保健 □药品和医疗器械 □文化 □广播电视节目 □电子公告服务 □其他
四、接入信息报备内容:
本单位是否正确报备接入信息(包括“接入服务提供者名称”、“接入方式”、“服务器放置地点”、“网站 IP 地址”) □是 □否
五、是否留存网站备案信息书面文档 □是 □否
网站备案信息核验承诺:(接入服务单位、网站主办者签署)
本单位(接入服务单位)已仔细阅读“《网站备案信息真实性核验单》填写说明”,对说明内容已全部知晓并充分了解,愿意遵守全部内容。承诺已对《网站备案信息真实性核验单》“网站备案信息核验内容”中包含的网站主办者提交主体信息、联系方式、网站信息,本单位报备的接入信息进行逐项核验;承诺以上核验记录真实有效。 核验人签字: 单位盖章(接入服务单位): 日 期: 年 月 日 - 本人(本单位)已履行网站备案信息当面核验手续,承认以上填写信息和核验记录真实有效,承诺上述备案信息一旦发生变更,将及时进行更新,并愿意承担因网站备案信息不准确或更新不及时而采取的停止网站接入服务、注销备案等相应处理措施。 网站负责人签字: 单位盖章(网站主办者): 日 期: 年 月 日

3.2.2 互联网运营单位管理

1. 管理依据

1)《中华人民共和国计算机信息系统安全保护条例》

第六条 公安部主管全国计算机信息系统安全保护工作。

2)《中华人民共和国计算机信息网络国际联网管理暂行规定》

第六条 计算机信息网络直接进行国际联网,必须使用邮电部国家公用电信网提供的国际出入口信道。

任何单位和个人不得自行建立或者使用其他信道进行国际联网。

第八条 接入网络必须通过互联网络进行国际联网。

接入单位拟从事国际联网经营活动的,应当报有权受理从事国际联网经营活动申请的

互联单位主管部门或者主管单位申请领取国际联网经营许可证；未取得国际联网经营许可证的，不得从事国际联网经营业务。

接入单位拟从事非经营活动的，应当报经有权受理从事非经营活动申请的互联单位主管部门或者主管单位审批；未经批准的，不得接入互联网络进行国际联网。

申请领取国际联网经营许可证或者办理审批手续时，应当提供其计算机信息网络的性质、应用范围和主机地址等资料。

国际联网经营许可证的格式，由国务院信息化工作领导小组统一制定。

第十条　个人、法人和其他组织（以下统称用户）使用的计算机或者计算机信息网络，需要进行国际联网的，必须通过接入网络进行国际联网。

前款规定的计算机或者计算机信息网络，需要接入网络的，应当征得接入单位的同意，并办理登记手续。

3）《计算机信息网络国际联网安全保护管理办法》

第三条　公安部计算机管理监察机构负责计算机信息网络国际联网的安全保护管理工作。公安机关计算机管理监察机构应当保护计算机信息网络国际联网的公共安全，维护从事国际联网业务的单位和个人的合法权益和公众利益。

第八条　从事国际联网业务的单位和个人应当接受公安机关的安全监督、检查和指导，如实向公安机关提供有关安全保护的信息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为。

第九条　国际出入口信道提供单位、互联单位的主管部门或者主管单位，应当依照法律和国家有关规定负责国际出入口信道、所属互联网络的安全保护管理工作。

第十五条　省、自治区、直辖市公安厅（局），地（市）、县（市）公安局，应当有相应机构负责国际联网的安全保护管理工作。

第十六条　公安机关计算机管理监察机构应当掌握互联单位、接入单位和用户的备案情况，建立备案档案，进行备案统计，并按照国家有关规定逐级上报。

第十七条　公安机关计算机管理监察机构应当督促互联单位、接入单位及有关用户建立健全安全保护管理制度。监督、检查网络安全保护管理以及技术措施的落实情况。

公安机关计算机管理监察机构在组织安全检查时，有关单位应当派人参加。公安机关计算机管理监察机构对安全检查发现的问题，应当提出改进意见，作出详细记录，存档备查。

2. 管理对象

互联网运营单位安全管理对象主要包括在中华人民共和国境内从事互联网接入、主机托管及租赁、空间租用、域名注册等互联网运营服务单位。

3. 管理与服务内容

（1）督促、指导互联网运营单位建立安全组织机构，落实安全管理人员，并报公安机关网络安全保卫部门备案。计算机安全组织负责指挥、组织、协调本单位的计算机信息系统安全保护工作，对本单位的计算机信息网络安全统一指导管理。安全组织要设立两名以上专

职安全员，安全员和计算机安全相关重要岗位的人员应当参加公安机关组织的安全培训，持证上岗。

（2）督促、指导互联网运营单位到公安机关网络安全保卫部门进行备案。互联网运营单位应当自网络开通之日起30日内到所在地公安机关网络安全保卫部门依法办理备案手续，并按照公安机关规定提交个人用户变更情况，协助公安机关开展个人用户的备案工作。

（3）督促、指导互联网运营单位履行告知新增的联网单位用户和开设网站、网页的联网个人用户到公安机关网络安全保卫部门进行备案的义务。

（4）督促、指导互联网运营单位完善具体网络服务项目、网络拓扑结构、上网接入方式（包括小区的接入方式及小区内的组网方式）、IP地址的分布及IP地址和用户对应等基本要求。

（5）督促、指导互联网运营单位建立健全安全保护管理制度，包括：

① 计算机机房安全保护管理制度。

② 安全管理责任人、信息审查员的任免和安全责任制度。

③ 网络安全漏洞检测和系统升级管理制度。

④ 操作权限管理制度。

⑤ 用户登记制度。

⑥ 异常情况及违法犯罪案件报告和协查制度。

⑦ 安全教育和培训制度。

⑧ 重要信息系统的系统备份及应急预案制度。

⑨ 备案制度。

（6）督促、指导互联网运营单位在实体安全、信息安全、运行安全和网络安全等方面采取必要的安全保护技术措施，包括：

① 系统时钟统一，采取核对北京时间措施。

② 系统重要部分的冗余或备份措施。

③ 计算机病毒防治措施。

④ 网络攻击防范、追踪措施。

⑤ 安全审计和预警措施。

⑥ 系统运行和用户使用日志记录保存60日以上措施。

⑦ 对使用公网动态IP地址上网的用户，上网日志应包括上网时间、下网时间、用户名、主叫电话号码、分配给用户的IP地址等信息。

⑧ 使用内部IP地址，通过网络地址转换技术（NAT）上网的用户，上网日志应包括上网时间、下网时间、用户名、网卡MAC地址、内部IP地址、内部IP地址与外部IP地址的对应关系、访问的目标IP地址等信息。

⑨ 身份登记和识别确认措施。

⑩ 使用有关国家规定的安全管理产品（硬件和软件）。

(7) 督促、指导互联网运营单位制定突发安全事件和事故的应急处置方案。

(8) 督促、指导互联网运营单位通过互联网络进行国际联网，不得以其他方式进入国际联网。

(9) 督促、指导互联网运营单位落实计算机有害数据过滤、报告制度。

(10) 督促、指导互联网运营单位提供安全保护管理所需信息、资料及数据文件，主要包括：

① 用户注册登记、使用与变更情况(含用户账号、IP 地址及用户个人备案资料等)。

② IP 地址分配、使用及变更情况。

③ 用户网络服务功能设置及变更情况。

④ 与安全保护工作相关的其他信息。

4. 工作方法和要求

(1) 全面掌握本地所有互联网运营单位的基本情况，积极发展安全组织机构和安全员，加强对安全负责人、安全联络员、安全专管员及相关技术人员的管理，建立安全组织人员资料库，及时掌握运营单位的运行情况。

(2) 全面掌握互联网运营单位网络拓扑结构的基本情况，要求运营单位向公安机关网络安全保卫部门提供本单位网络拓扑结构的三级网络示意图。

(3) 全面掌握互联网运营单位 IP 资源和 IP 资源的分配接入方式(包括小区的接入方式、小区内的组网方式、IP 地址的分配和使用情况)，将 IP 资源情况录入基础数据库。

(4) 全面掌握互联网运营单位网络出口情况，重点发现互联网运营单位私自接入互联网或使用异地网络出口的情况，有效避免出现监管漏洞。

(5) 加强安全保护技术措施的检查，重点检查安全审计技术措施落实情况，对提供拨号上网、无线上网或小区接入的单位，着重要求采取必要的技术措施实现上网 IP、上网时间与上网用户的一一对应关系；特别是针对采用 NAT 方式为用户提供上网服务的单位，务必要求其记录 NAT 转换记录(包括内网 IP、转换出口的公网 IP、时间、访问的目的地址等)。

(6) 督促互联网运营单位依法履行备案义务和通知其提供服务的联网用户办理备案手续，并按照要求做好定期数据报送。在规定期间向公安机关网络安全保卫部门报送本月新增和变更的用户资料以及本单位 IP 地址使用情况，及时将报送数据整理录入基础数据库。

(7) 统一向互联网运营单位提供固定的报送接口和报送格式，不得随意改变报送接口和报送格式。

(8) 定期走访运营单位，每半年至少到各个单位走访调研一次，及时了解各单位发展情况和业务发展计划。

(9) 对未落实安全保护管理制度，经常发生违法行为，或未落实案件协查制度，案件倒查准确率不足 95%的，经屡次教育坚决不予改正的互联网运营单位严格依法查处。

5. 行政处罚

(1)《计算机信息网络国际联网安全保护管理办法》。

第二十一条　有下列行为之一的,由公安机关责令限期改正,给予警告,有违法所得的,没收违法所得;在规定的限期内未改正的,对单位的主管负责人员和其他直接责任人员可以并处五千元以下的罚款,对单位可以并处一万五千元以下的罚款;情节严重的,并可以给予六个月以内的停止联网、停机整顿的处罚,必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格。

① 未建立安全保护管理制度的。

② 未采取安全技术保护措施的。

③ 未对网络用户进行安全教育和培训的。

④ 未提供安全保护管理所需信息、资料及数据文件,或者所提供内容不真实的。

⑤ 对委托其发布的信息内容未进行审核或者对委托单位和个人未进行登记的。

⑥ 未建立电子公告系统的用户登记和信息管理制度的。

⑦ 未按照国家有关规定,删除网络地址、目录或者关闭服务器的。

⑧ 未建立公用账号使用登记制度的。

⑨ 转借、转让用户账号的。

(2) 不履行备案职责的,根据《计算机信息网络国际联网安全保护管理办法》第二十三条规定,由公安机关给予警告或者停机整顿不超过六个月的处罚。

(3) 根据《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》第二十二条规定,对未使用邮电部国家公用电信网提供的国际出入口信道,或自行建立或者使用其他信道进行国际联网的,由公安机关责令停止联网,可以并处一万五千元以下罚款;有违法所得的,没收违法所得。对接入单位未领取国际联网经营许可证从事国际联网经营活动的,由公安机关给予警告,限期办理经营许可证;在限期内不办理经营许可证的,责令停止联网;有违法所得的,没收违法所得。对个人、法人和其他组织用户未通过接入网络进行国际联网的,对个人由公安机关处五千元以下的罚款;对法人和其他组织用户由公安机关给予警告,可以并处一万五千元以下的罚款。对进行国际联网的专业计算机信息网络经营国际互联网络业务的,由公安机关给予警告,可以并处一万五千元以下的罚款;有违法所得的,没收违法所得。企业计算机信息网络和其他通过专线进行国际联网的计算机信息网络违反只限于内部使用规定的,由公安机关给予警告,可以并处一万五千元以下的罚款;有违法所得的,没收违法所得。

6. 工作流程

1) 日常管理工作流程

互联网运营单位日常管理工作流程如图 3-3 所示。

2) 日常检查工作流程

互联网运营单位日常检查工作流程如图 3-4 所示。

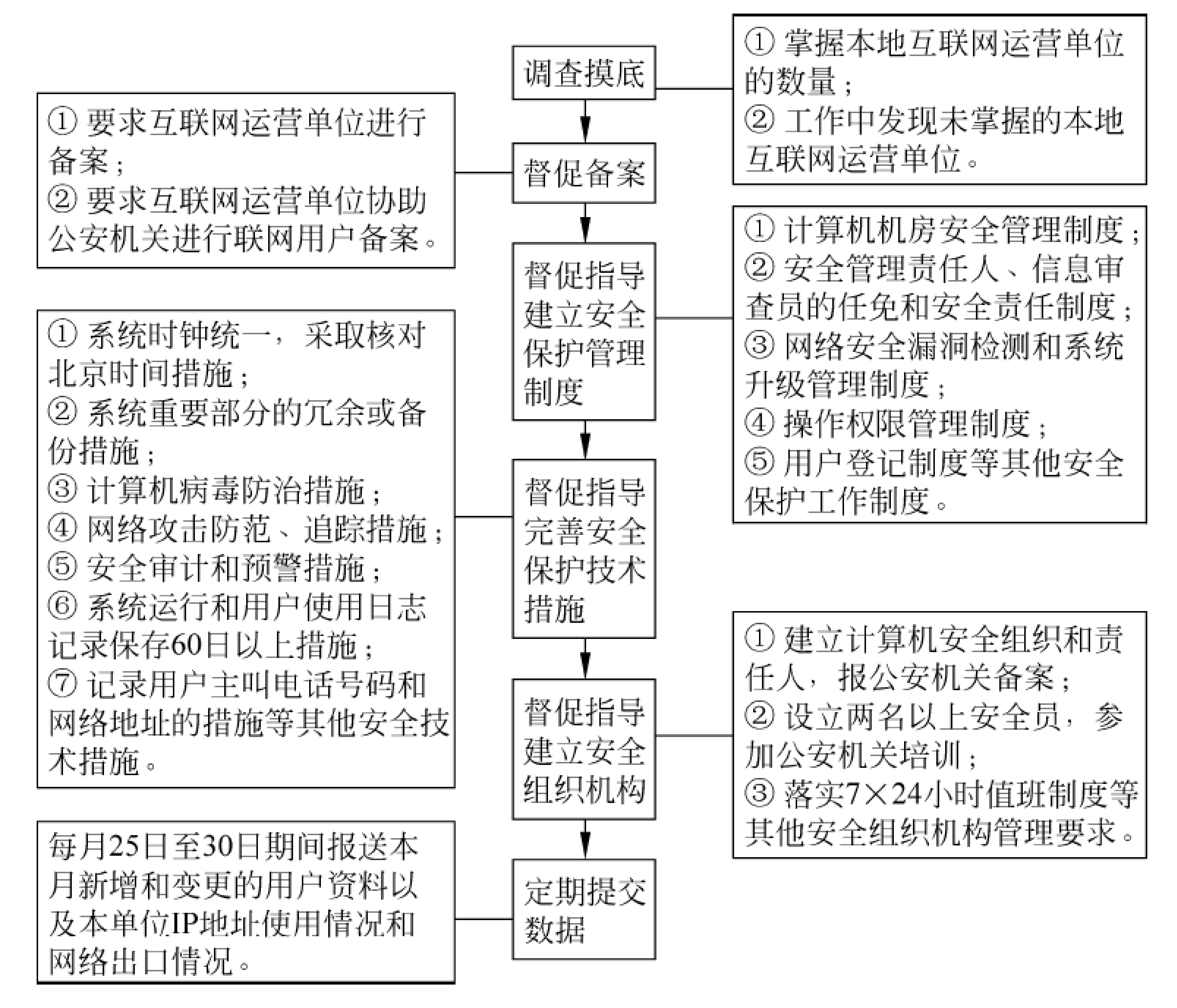


图 3-3　互联网运营单位日常管理工作流程

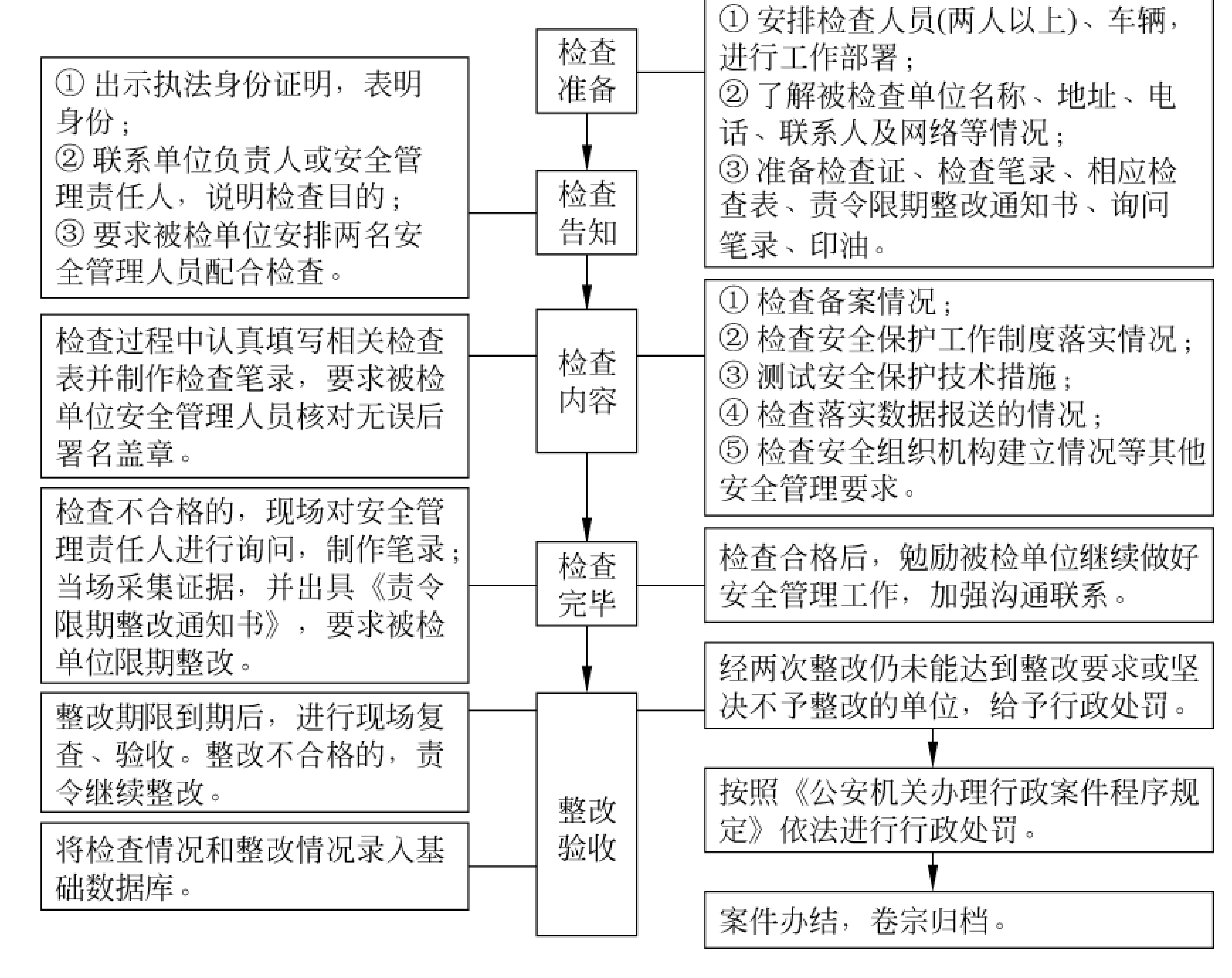


图 3-4　互联网运营单位日常检查工作流程

7. 相关表格

××市公共信息网络运营单位安全检查表

检查单位：××市公安局公共信息网络安全保卫部门

时间：　年　月　日

被检查单位		经营业务范围		
单位地址		邮政编码		
单位负责人		联系电话		
安全员		联系电话		
安全管理制度	1. 有无建立计算机机房安全保护管理制度			有□无□
	2. 有无建立安全管理责任人、信息审查员的任免和安全责任制度			有□无□
	3. 有无建立网络安全漏洞检测和系统升级管理制度			有□无□
	4. 有无建立操作权限管理制度			有□无□
	5. 有无建立用户登记制度			有□无□
	6. 有无建立病毒检测和网络安全漏洞检测制度			有□无□
	7. 有无建立违法案件报告协助查处制度			有□无□
	8. 有无建立账号使用登记和操作权限管理制度			有□无□
	9. 有无建立安全教育培训制度			有□无□
	10. 有无依法办理备案			有□无□
安全保护技术措施	11. 有无建立系统重要部分的冗余或备份措施			有□无□
	12. 有无建立计算机病毒防治措施，使用何种计算机防病毒软件			有□无□
	13. 有无建立网络攻击防范、追踪措施			有□无□
	14. 有无建立安全审计和预警措施			有□无□
	15. 系统各部位时钟是否以北京时间为标准统一			是□否□
	16. 有无系统运行和用户使用日志记录			有□无□
	17. 系统运行和用户使用日志记录有无保存 60 日以上			有□无□
	18. 有无记录用户主叫电话号码和网络地址的措施			有□无□
	19. 有无身份登记和识别确认措施			有□无□
	20. 是否使用国家规定的安全管理产品（硬件和软件）			有□无□
	21. 有无制定应急方案			有□无□
	22. 有无措施定期进行计算机信息网络风险评估，及时发现信息系统安全隐患并采取整改			有□无□
	23. 有无记录 ISDN、ADSL 等各类拨号上网用户的主叫号码、网络地址			有□无□
	24. 有无记录发生案件、事故和发现计算机有害数据的情况			有□无□
安全责任书	有无与公安机关签订有关网络与信息安全责任书，落实“谁主管、谁负责”的安全责任制度			有□无□
IP 地址段范围				

续表

提供安全保护管理所需信息、资料及数据文件情况	用户注册登记、使用与变更情况（含用户账号、IP 与 E-mail 地址等）	
	IP 地址分配、使用及变更情况	
	网络服务功能设置情况	
	与安全保护工作相关的其他信息	
用户备案情况		
计算机信息网络安全事件、事故报告制度落实情况		
安全领导小组和安全员名单及联系电话		

检查民警：　　　　　　　　　　　　　　　　　联系电话：

被检查单位负责人：

安全员或技术员：

（盖章）

检查日期：　年　月　日

互联网信息安全责任书

管理监察单位：××市公安局公共信息网络安全保卫支队

责任单位：

为了明确各互联网数据中心（IDC）和开展虚拟主机业务的单位所应履行的安全管理责任，进一步规范互联网数据中心（IDC）和开展虚拟主机业务的单位的经营行为，确保互联网络与信息安全，同时也为客户营造一个安全洁净的网络环境，根据《计算机信息网络国际联网安全保护管理办法》等有关法律法规的规定，责任单位将认真落实如下责任：

一、自觉遵守法律、行政法规和其他有关规定，接受公安机关的安全监督、检查和指导，如实向公安机关提供有关安全保护的信息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为。

二、不利用国际联网危害国家安全，泄露国家秘密，不侵犯国家的、社会的、集体的利益和公民的合法权益，不从事违法犯罪活动。

三、不利用国际联网制作、复制、查阅和传播下列信息：

（一）煽动抗拒、破坏宪法和法律、行政法规实施的；

（二）煽动颠覆国家政权，推翻社会主义制度；

（三）煽动分裂国家、破坏国家统一；
（四）煽动民族仇恨、民族歧视，破坏民族团结；
（五）捏造或歪曲事实，散布谣言，扰乱社会秩序；
（六）宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的；
（七）公然侮辱他人或者捏造事实诽谤他人的；
（八）损害国家机关信誉的；
（九）其他违反宪法和法律、行政法规的。

四、不从事下列危害计算机信息网络安全的活动：
（一）未经允许，进入计算机信息网络或者使用计算机信息网络资源的；
（二）未经允许，对计算机信息网络功能进行删除、修改或者增加的；
（三）未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的；
（四）故意制作、传播计算机病毒等破坏性程序的；
（五）其他危害计算机信息网络安全的。

五、建立安全保护管理制度，落实各项安全保护技术措施，保障本单位网络运行安全和信息安全。

六、严格按照国家相关的法律法规做好本单位网络的信息安全管理工作，设立信息安全责任人和信息安全审查员，信息安全责任人和信息安全审查员在参加××市公安局网安支队认可的安全技术培训后，持证上岗。每月由信息安全审查员定期对本单位的接入用户及主机托管用户、主机租用用户、虚拟主机用户的安全审计日志及信息发布内容进行检查，发现有以上二、三、四点所列情形之一的，应当保留有关原始记录，并在 24 小时内向公安网络安全保卫部门报告。

七、按照国家有关规定，删除本单位网络中含有以上第三点内容地址、目录或关闭服务器。

八、与本单位所属接入用户及主机租用、托管用户和虚拟主机用户签订互联网信息安全承诺书，明确其责任、规范其管理维护行为。

九、对本单位接入用户及主机托管、主机租用和虚拟主机的用户应采用实名登记，并将用户变更情况于每月 25 日前报送公安网安部门。

十、变更名称、住所、法定代表人或者主要负责人、网络资源或者终止经营活动，到公安机关办理有关手续或者备案。

十一、本责任书自签署之日起生效。

责任单位（盖章）：
法人代表（签字）：
年　月　日

互联网信息安全承诺书

一、本单位(或个人)因为("□"为选项):

□使用____________________的互联网络资源;

□与____________________开展其他互联网合作项目。

郑重承诺遵守本承诺书的有关条款,如有违反本承诺书有关条款的行为,由本单位(或个人)承担由此带来的一切民事、行政和刑事责任。

二、本单位(或个人)承诺遵守《中华人民共和国计算机信息系统安全保护条例》和《计算机信息网络国际联网安全保护管理办法》等国家的有关法律、法规和行政规章制度。

本单位(或个人)开设的网站,在开通联网的 30 天内到××市公安局网安部门履行备案手续,并将接受××市公安局网安部门的监督和检查,如实主动提供有关安全保护的信息、资料及数据文件,积极协助查处通过国际联网的计算机信息网络违法犯罪行为。

三、本单位(或个人)保证不利用国际互联网危害国家安全、泄露国家秘密,不侵犯国家的、社会的、集体的利益和公民的合法权益,不从事违法犯罪活动。

四、本单位(或个人)承诺严格按照国家相关的法律法规做好网站的信息安全管理工作,设立信息安全责任人和信息安全审查员,信息安全责任人和信息安全审查员在参加××市公安局网络安全保卫部门认可的安全技术培训后,持证上岗。

本单位(或个人)承诺健全各项互联网安全保护管理制度和落实各项安全保护技术措施。

五、本单位(或个人)承诺不制作、复制、查阅和传播不列信息:

(一) 反对宪法所确定的基本原则的;

(二) 危害国家安全,泄露国家秘密,颠覆国家政权,破坏国家统一的;

(三) 损害国家荣誉和利益的;

(四) 煽动民族仇恨、民族歧视,破坏民族团结的;

(五) 破坏国家宗教政策,宣扬邪教和封建迷信的;

(六) 散布谣言,扰乱社会秩序,破坏社会稳定的;

(七) 散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的;

(八) 侮辱或者诽谤他人,侵害他人合法权益的;

(九) 含有法律、行政法规禁止的其他内容的。

六、本单位(或个人)承诺不从事下列危害计算机信息网络安全的活动:

(一) 未经允许,进入计算机信息网络或者使用计算机信息网络资源的;

(二) 未经允许,对计算机信息网络功能进行删除、修改或者增加的;

(三) 未经允许,对计算机信息网络中存储或者传输的数据和应用程序进行删除、修改或者增加的;

(四) 故意制作、传播计算机病毒等破坏性程序的;

(五) 其他危害计算机信息网络安全的。

七、本单位(或个人)承诺当计算机信息系统发生重大安全事故时,立即采取应急措施,保留有关原始记录,并在24小时内向××市公安局网络安全保卫部门报告。

八、若违反本承诺书有关条款和国家相关法律法规的,本单位(或个人)直接承担相应法律责任;造成第三方财产损失的,本单位(或个人)将在国家有关机关确认的责任范围内直接赔偿。

九、本承诺书自签署之日起施行。

责任单位(或个人):

法人代表(或授权代表):

二〇　年　月

3.2.3 互联网信息服务单位管理

1. 管理依据

1)《计算机信息网络国际联网安全保护管理办法》

第五条　任何单位和个人不得利用国际联网制作、复制、查阅和传播下列信息:

① 煽动抗拒、破坏宪法和法律、行政法规实施的;

② 煽动颠覆国家政权,推翻社会主义制度的;

③ 煽动分裂国家、破坏国家统一的;

④ 煽动民族仇恨、民族歧视,破坏民族团结的;

⑤ 捏造或者歪曲事实,散布谣言,扰乱社会秩序的;

⑥ 宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖,教唆犯罪的;

⑦ 公然侮辱他人或者捏造事实诽谤他人的;

⑧ 损害国家机关信誉的;

⑨ 其他违反宪法和法律、行政法规的。

第六条　任何单位和个人不得从事下列危害计算机信息网络安全的活动:

① 未经允许,进入计算机信息网络或者使用计算机信息网络资源的;

② 未经允许,对计算机信息网络功能进行删除、修改或者增加的;

③ 未经允许,对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的;

④ 故意制作、传播计算机病毒等破坏性程序的;

⑤ 其他危害计算机信息网络安全的。

第七条　用户的通信自由和通信秘密受法律保护。任何单位和个人不得违反法律规定,利用国际联网侵犯用户的通信自由和通信秘密。

第十条　互联单位、接入单位及使用计算机信息网络国际联网的法人和其他组织应当履行下列安全保护职责:

① 负责本网络的安全保护管理工作,建立健全安全保护管理制度;

② 落实安全保护技术措施,保障本网络的运行安全和信息安全;

③ 负责对本网络用户的安全教育和培训;

④ 对委托发布信息的单位和个人进行登记,并对所提供的信息内容按照本办法第五条进行审核;

⑤ 建立计算机信息网络电子公告系统的用户登记和信息管理制度;

⑥ 发现有本办法第四条、第五条、第六条、第七条所列情形之一的,应当保留有关原始记录,并在二十四小时内向当地公安机关报告;

⑦ 按照国家有关规定,删除本网络中含有本办法第五条内容的地址、目录或者关闭服务器。

第十二条　互联单位、接入单位、使用计算机信息网络国际联网的法人和其他组织(包括跨省、自治区、直辖市联网的单位和所属的分支机构),应当自网络正式联通之日起三十日内,到所在地的省、自治区、直辖市人民政府公安机关指定的受理机关办理备案手续。

前款所列单位应当负责将接入本网络的接入单位和用户情况报当地公安机关备案,并及时报告本网络中接入单位和用户的变更情况。

第十七条　公安机关计算机管理监察机构应当督促互联单位、接入单位及有关用户建立健全安全保护管理制度。监督、检查网络安全保护管理以及技术措施的落实情况。

公安机关计算机管理监察机构在组织安全检查时,有关单位应当派人参加。公安机关计算机管理监察机构对安全检查发现的问题,应当提出改进意见,作出详细记录,存档备查。

2)《互联网信息服务管理办法》

第十四条　从事新闻、出版以及电子公告等服务项目的互联网信息服务提供者,应当记录提供的信息内容及其发布时间、互联网地址或者域名;互联网接入服务提供者应当记录上网用户的上网时间、用户账号、互联网地址或者域名、主叫电话号码等信息。

互联网信息服务提供者和互联网接入服务提供者的记录备份应当保存 60 日,并在国家有关机关依法查询时,予以提供。

第十五条　互联网信息服务提供者不得制作、复制、发布、传播含有下列内容的信息:

① 对宪法所确定的基本原则的;

② 危害国家安全,泄露国家秘密,颠覆国家政权,破坏国家统一的;

③ 损害国家荣誉和利益的;

④ 煽动民族仇恨、民族歧视,破坏民族团结的;

⑤ 破坏国家宗教政策,宣扬邪教和封建迷信的;

⑥ 散布谣言,扰乱社会秩序,破坏社会稳定的;

⑦ 散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的;

⑧ 侮辱或者诽谤他人,侵害他人合法权益的;

⑨ 含有法律、行政法规禁止的其他内容的。

第十六条　互联网信息服务提供者发现其网站传输的信息明显属于本办法第十五条所列内容之一的,应当立即停止传输,保存有关记录,并向国家有关机关报告。

2. 管理种类

互联网信息服务单位管理包括网站、电子邮件服务单位、互联网娱乐平台服务单位、点对点信息服务单位、网上短消息服务单位及网上公共信息场所等单位的管理。

互联网信息服务分为经营性和非经营性两类。非经营性互联网信息服务单位是指通过互联网向用户无偿提供具有公开性、共享性信息服务活动。主要是指各级政府部门的网站、新闻机构的电子版报刊，企事业单位、教育科研机构的各类公益性网站和对本单位产品或业务作自我宣传的网站。经营性互联网信息服务单位是指通过互联网，向上网用户有偿提供信息或者网页制作等服务活动。经营的内容主要是网上广告、代制作网页、服务器内存空间出租、有偿提供特定信息内容、电子商务及其他网上应用服务。国家对经营性互联网信息服务单位实行经营许可证制度，对非经营性 ICP 实行备案制度。

3. 管理对象

(1) 网站安全管理对象包括中华人民共和国境内的网站开设单位。

(2) 电子邮件安全管理对象包括中华人民共和国境内的电子邮件服务单位。

(3) 互联网娱乐平台安全管理对象是中华人民共和国境内以公共信息网络为平台，发行、运营互联网网络游戏的单位和互联网网络游戏开发、代理、运营单位。

(4) 点对点信息安全管理对象是中华人民共和国境内，以点对点共享网络为平台进行点对点文件共享和数据交互以及其他点对点信息应用的单位。

(5) 互联网短信息服务安全管理对象是中华人民共和国境内以移动通信运营商和互联网信息服务单位提供的信息交换平台，进行文字、图片等短信息交流的单位。

(6) 网上公共信息场所管理对象是指通过互联网向上网用户提供信息或者电子公告、BBS、论坛、网络聊天室、网页制作、即时通信等交互形式，为上网用户提供信息发布条件，为市民提供信息公共场所的单位。

4. 管理和服务的内容

(1) 督促、指导互联网信息服务单位建立安全组织机构，落实安全管理人员。

(2) 督促、指导互联网信息服务单位到公安机关网络安全保卫部门依法履行备案义务。

(3) 督促、指导互联网信息服务单位建立健全安全保护管理制度。

(4) 督促、指导互联网信息服务单位完善落实安全保护技术措施。

(5) 督促、指导电子邮件服务单位建立健全邮件服务工作规范。

(6) 督促、指导网络娱乐平台服务单位、点对点信息服务运营单位与公安机关信息网络安全报警处置系统连接，实现用户账号等报警特征条件和有害信息过滤关键词远程更新，用户信息和留存信息远程查询。

(7) 督促、指导点对点信息服务运营单位关闭或删除含有有害信息的地址、目录或者服务器；对传播有害信息的用户基于用户账号、网络地址进行屏蔽。

(8) 督促、指导点对点信息服务运营单位与公安机关网络安全保卫部门建立网上违法犯罪案件协助配合调查的工作程序。

5. 工作方法和要求

(1) 全面掌握基本情况。

(2) 加强安全检查和指导。

(3) 建立日常应急联络机制。

(4) 逐步落实实名制。

(5) 督促、指导网站落实信息先审后发制度。

(6) 督促、指导电子邮件服务单位落实关键字技术措施；推动电子邮件服务单位履行行业规范；建立案件协查机制；建立有害信息的应急处置机制。

(7) 加强对互联网娱乐平台开设的新业务、新栏目指导监管，防止涉及黄赌毒内容的业务进入互联网娱乐平台；落实重点网络游戏用户虚拟财产保护工作；加强对互联网娱乐平台的公示牌聊天功能等交互式空间内容的管理。

(8) 建立紧急突发事件预警通报机制。

6. 行政处罚

(1) 根据《计算机信息网络国际联网安全保护管理办法》第二十条规定，利用国际联网制作、复制、查阅和传播有害信息或者从事危害计算机信息网络安全活动的，由公安机关给予警告，有违法所得的，没收违法所得，对个人可以并处五千元以下的罚款，对单位可以并处一万五千元以下的罚款；情节严重的，并可以给予六个月以内停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格；构成违反治安管理行为的，依照治安管理处罚条例的规定处罚；构成犯罪的，依法追究刑事责任。

(2) 根据《计算机信息网络国际联网安全保护管理办法》第二十一条规定，有下列行为之一的，由公安机关责令限期改正，给予警告，有违法所得的，没收违法所得；在规定的限期内未改正的，对单位的主管负责人员和其他直接责任人员可以并处五千元以下的罚款，对单位可以并处一万五千元以下的罚款；情节严重的，并可以给予六个月以内的停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格。

① 未建立安全保护管理制度的。

② 未采取安全技术保护措施的。

③ 未对网络用户进行安全教育和培训的。

④ 未提供安全保护管理所需信息、资料及数据文件，或者所提供内容不真实的。

⑤ 对委托其发布的信息内容未进行审核或者对委托单位和个人未进行登记的。

⑥ 未建立电子公告系统的用户登记和信息管理制度的。

⑦ 未按照国家有关规定，删除网络地址、目录或者关闭服务器的。

⑧ 未建立公用账号使用登记制度的。

⑨ 转借、转让用户账号的。

(3) 根据《计算机信息网络国际联网安全保护管理办法》第二十三条规定，不履行备案职责的，由公安机关给予警告或者停机整顿不超过六个月的处罚。

（4）根据《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》第二十二条规定，对未使用邮电部国家公用电信网提供的国际出入口信道，或自行建立或者使用其他信道进行国际联网的，由公安机关责令停止联网，可以并处一万五千元以下罚款；有违法所得的，没收违法所得。对接入单位未领取国际联网经营许可证从事国际联网经营活动的，由公安机关给予警告，限期办理经营许可证；在限期内不办理经营许可证的，责令停止联网；有违法所得的，没收违法所得。对个人、法人和其他组织用户未通过接入网络进行国际联网的，对个人由公安机关处五千元以下的罚款；对法人和其他组织用户由公安机关给予警告，可以并处一万五千元以下的罚款。对进行国际联网的专业计算机信息网络经营国际互联网络业务的，由公安机关给予警告，可以并处一万五千元以下的罚款；有违法所得的，没收违法所得。企业计算机信息网络和其他通过专线进行国际联网的计算机信息网络违反只限于内部使用规定的，由公安机关给予警告，可以并处一万五千元以下的罚款；有违法所得的，没收违法所得。

7. 工作流程

1）日常管理工作流程

互联网信息服务单位日常管理工作流程如图 3-5 所示。

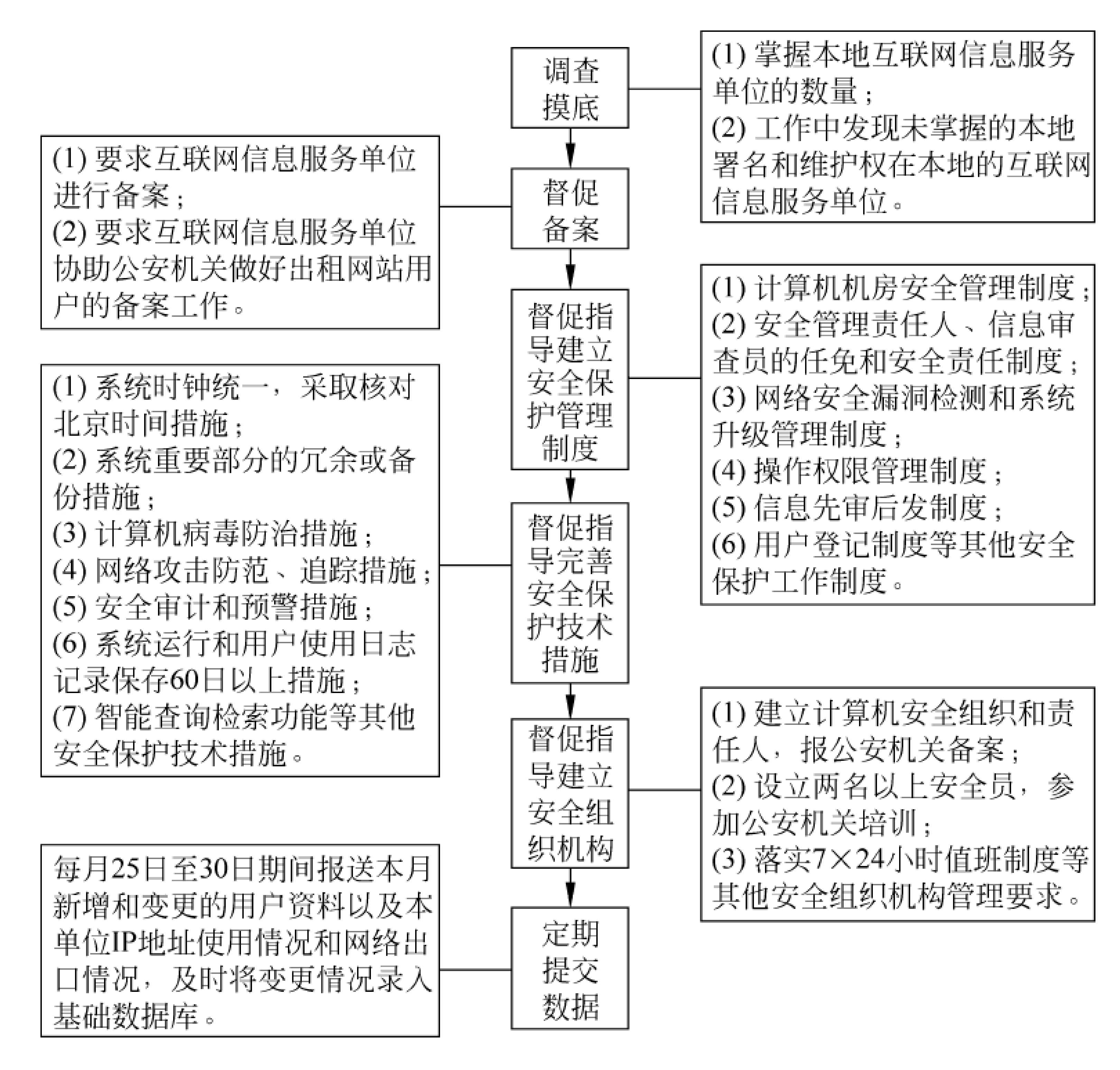


图 3-5 互联网信息服务单位日常管理工作流程

2）日常检查工作流程

互联网信息服务单位日常检查工作流程参见如图 3-4 所示的互联网运营单位日常检查工作流程。

8. 相关表格

××市信息网络应用单位网络安全检查表

检查单位：××市公安局公共信息网络安全保卫支队　　　　　　时间：　年　月　日

<table>
<tr><td>被检查单位名称</td><td colspan="3"></td></tr>
<tr><td>单位地址</td><td colspan="3"></td></tr>
<tr><td>负责人</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>联网情况</td><td>接入方式(服务商)________
账号(电话)________
联网主机数________
IP 地址________
服务内容________
联网用途________</td><td colspan="2">网络拓扑图</td></tr>
<tr><td rowspan="4">组织制度</td><td colspan="2">单位成立网络安全小组，确立安全小组责任人(单位领导任组长)，确立组长责任制</td><td>有□　无□</td></tr>
<tr><td colspan="2">组长落实小组人员岗位工作职责</td><td>有□　无□</td></tr>
<tr><td colspan="2">配备 2～4 名计算机安全员，须持证上岗</td><td>有□　无□</td></tr>
<tr><td colspan="2">制定网络安全事故处置措施</td><td>有□　无□</td></tr>
<tr><td rowspan="8">安全保护管理制度</td><td colspan="2">计算机机房安全保护管理制度</td><td>有□　无□</td></tr>
<tr><td colspan="2">用户登记制度和操作权限管理制度</td><td>有□　无□</td></tr>
<tr><td colspan="2">网络安全漏洞检测和系统升级管理制度</td><td>有□　无□</td></tr>
<tr><td colspan="2">交互式栏目 24 小时巡查制度</td><td>有□　无□</td></tr>
<tr><td colspan="2">电子公告系统用户登记制度</td><td>有□　无□</td></tr>
<tr><td colspan="2">信息发布审核、登记、保存、清除和备份制度，信息群发服务管理制度</td><td>有□　无□</td></tr>
<tr><td colspan="2">违法案件报告和协查制度</td><td>有□　无□</td></tr>
<tr><td colspan="2">备案制度</td><td>有□　无□</td></tr>
<tr><td rowspan="8">安全保护技术措施</td><td colspan="2">具有保存 3 个月以上系统网络运行日志和用户使用日志记录功能，内容包括 IP 地址分配及使用情况，交互式信息发布者、主页维护者、邮箱使用者和拨号用户上网的起止时间和对应 IP 地址，交互式栏目的信息等</td><td>有□　无□</td></tr>
<tr><td colspan="2">安全审计及预警措施</td><td>有□　无□</td></tr>
<tr><td colspan="2">网络攻击防范、追踪措施</td><td>有□　无□</td></tr>
<tr><td colspan="2">计算机病毒防治措施</td><td>有□　无□</td></tr>
<tr><td colspan="2">身份登记和识别确认措施</td><td>有□　无□</td></tr>
<tr><td colspan="2">交互式栏目具有关键字过滤技术措施</td><td>有□　无□</td></tr>
<tr><td colspan="2">开设短信息服务的具有短信群发限制、过滤和删除等技术措施</td><td>有□　无□</td></tr>
<tr><td colspan="2">开设邮件服务的，是否具有垃圾邮件的清理功能</td><td>是□　否□</td></tr>
<tr><td colspan="4">检查意见：</td></tr>
</table>

检查民警：　　　　　　　　　　　　　　被检查单位负责人：

××市互联网电子邮件服务安全检查表

检查单位：××市公安局公共信息网络安全保卫支队　　　　时间：　年　月　日

<table>
<tr><td>单位名称</td><td></td><td>负责人</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>单位地址</td><td></td><td>邮件服务管理人</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>联网方式</td><td colspan="4">□ADSL　□ISDN　□DDN
□微波　□HFC　□光纤</td><td>有（　　）个接入 IP</td></tr>
<tr><td>（固定 IP）互联网接入 IP 地址</td><td colspan="3"></td><td>所属 ISP</td><td></td></tr>
<tr><td>（动态 IP）互联网接入账号</td><td colspan="3"></td><td>上网电话</td><td></td></tr>
<tr><td>网站名称</td><td colspan="2"></td><td>网站 URL</td><td colspan="2"></td></tr>
<tr><td>电子邮件服务器 IP 地址</td><td></td><td rowspan="2">用户数量</td><td colspan="3">外：</td></tr>
<tr><td>使用的电子邮件服务软件</td><td></td><td colspan="3">内：</td></tr>
<tr><td rowspan="6">安全管理制度</td><td colspan="4">是否到公安机关履行备案手续</td><td>是□　否□</td></tr>
<tr><td colspan="4">有无设立有害垃圾电子邮件举报、投诉信箱</td><td>有□　无□</td></tr>
<tr><td colspan="4">有无建立用户举报、投诉处理制度</td><td>有□　无□</td></tr>
<tr><td colspan="4">有无设立反有害垃圾邮件公告信息</td><td>有□　无□</td></tr>
<tr><td colspan="4">有无建立与公安机关联系、报告制度</td><td>有□　无□</td></tr>
<tr><td colspan="4">有无保留备份有害垃圾电子邮件地址和相关记录</td><td>有□　无□</td></tr>
<tr><td rowspan="14">技术防范措施</td><td colspan="4">是否限制本地电子邮件用户一次性发送 25 封以上电子邮件（除特定用户外）</td><td>是□　否□</td></tr>
<tr><td colspan="4">有无本地邮件服务器电子邮件用户账号认证功能</td><td>有□　无□</td></tr>
<tr><td colspan="4">是否限制邮件服务器自动转发功能（除特定电子邮件外）</td><td></td></tr>
<tr><td colspan="4">有无保留电子邮箱用户登录、退出等日志记录 60 天</td><td>有□　无□</td></tr>
<tr><td colspan="4">是否能够对发送电子邮件的特定 IP 地址进行阻断</td><td>是□　否□</td></tr>
<tr><td colspan="4">是否能够限制来自相同客户端 IP 的最大同时连接数量、最大连接频率</td><td>是□　否□</td></tr>
<tr><td colspan="4">是否能够对电子邮件信头主题、收发件人、抄送人等内容进行基于特征字符串的过滤</td><td>是□　否□</td></tr>
<tr><td colspan="4">是否能够对电子邮件信体内容进行基于特征字符串的过滤</td><td>是□　否□</td></tr>
<tr><td colspan="4">是否能够对电子邮件附件标题、文件类型和长度进行基于特征字符串的过滤</td><td>是□　否□</td></tr>
<tr><td colspan="4">有无对符合过滤规则的电子邮件可以采用弹回、丢弃、转发、投递、等待、延时等动作</td><td>有□　无□</td></tr>
<tr><td colspan="4">是否支持过滤规则动态导入和维护，并立即生效</td><td>是□　否□</td></tr>
<tr><td colspan="4">是否对电子邮件信头、信体进行扫面之前，支持 BASE64 和 QuotedPrintable 等解码</td><td>是□　否□</td></tr>
<tr><td colspan="4">有无对有害垃圾电子邮件过滤和阻断数量进行统计的功能</td><td>有□　无□</td></tr>
<tr><td colspan="4">对公安机关所要求过滤的有害信息是否可以向公安机关远程传送</td><td>是□　否□</td></tr>
<tr><td colspan="6">检查结果：</td></tr>
</table>

检查民警：　　　　　　　　　　　　被检查单位负责人：

××市网络游戏运营单位安全检查表

检查单位：××市公安局公共信息网络安全保卫支队　　　　　　时间：　年　月　日

<table>
<tr><td>单位名称</td><td></td><td>负责人</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>单位地址</td><td></td><td>游戏运营管理人</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>公司业务</td><td colspan="5"></td></tr>
<tr><td>网站名称</td><td colspan="2"></td><td>网站 URL</td><td colspan="2"></td></tr>
<tr><td>游戏网站及服务器接入 IP 地址</td><td colspan="3"></td><td colspan="2">所属 ISP</td></tr>
<tr><td>游戏网站及服务器分布情况</td><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td rowspan="9">安全管理制度</td><td colspan="4">是否到公安机关履行备案手续</td><td>是□　否□</td></tr>
<tr><td colspan="4">有无建立与公安机关联系、报告制度</td><td>有□　无□</td></tr>
<tr><td colspan="4">有无建立违法案件报告和协查制度</td><td>有□　无□</td></tr>
<tr><td colspan="4">有无设立安全组织</td><td>有□　无□</td></tr>
<tr><td colspan="4">有无建立安全管理人员岗位工作职责</td><td>有□　无□</td></tr>
<tr><td colspan="4">有无安全教育和培训制度</td><td>有□　无□</td></tr>
<tr><td colspan="4">有无建立突发事件应急计划</td><td>有□　无□</td></tr>
<tr><td colspan="4">有无制定信息发布审核、登记制度</td><td>有□　无□</td></tr>
<tr><td colspan="4">有无落实病毒检测和网络安全漏洞检测制度</td><td>有□　无□</td></tr>
<tr><td rowspan="5">技术防范措施</td><td colspan="4">有无保存系统网络运行日志和用户使用日志记录 60 天以上</td><td>有□　无□</td></tr>
<tr><td colspan="4">有无保存游戏用户注册登记、使用与变更情况</td><td>有□　无□</td></tr>
<tr><td colspan="4">有无记录、保存游戏用户注册 IP 地址与登录 IP 地址</td><td>有□　无□</td></tr>
<tr><td colspan="4">有无落实游戏用户身份审计和在线监控措施</td><td>有□　无□</td></tr>
<tr><td colspan="4">有无对在线聊天采取关键字过滤技术</td><td>有□　无□</td></tr>
<tr><td rowspan="4">其他安全管理制度和技术措施</td><td colspan="4"></td><td></td></tr>
<tr><td colspan="4"></td><td></td></tr>
<tr><td colspan="4"></td><td></td></tr>
<tr><td colspan="4"></td><td></td></tr>
<tr><td rowspan="8">网络游戏运营情况</td><td colspan="2">网络游戏种类</td><td colspan="2">游戏名称</td><td>用户数量</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="6">检查结果：</td></tr>
</table>

检查民警：　　　　　　　　　　　　　　　　被检查单位负责人：

××市互联网信息服务单位安全检查表

检查单位：××市公安局公共信息网络安全保卫支队　　　　时间：　年　月　日

被检查单位		经营业务范围	
单位地址		邮政编码	
单位负责人		联系电话	
安全员		联系电话	
网站中文名		IP 地址	
网址			
设置的网络服务栏目	论坛□ 留言板□ 聊天室□ 即时通信□ 电子邮件□ 网页制作□ P2P□ 短信息□ 新闻□ 短信息□ 网络游戏□ 电子商务□ 空间出租□ 域名服务□ 搜索引擎□		
安全管理制度	1. 网站是否在公安部门备案		有□ 无□
	2. 有无建立本单位网络安全管理负责人和安全领导小组负责制度		有□ 无□
	3. 安全员、信息员是否经过培训持公安部门合格证上岗		有□ 无□
	4. 新闻网站和具有新闻登载资格的非新闻单位网站对新闻栏目有无实行先审后发制度		有□ 无□
	5. 有无对 BBS 栏目实行先审后发制度		有□ 无□
	6. 有无对新闻编辑人员实行资格认证和岗位责任制		有□ 无□
	7. 有无建立链接网站和聊天室等有害信息的检查管理制度		有□ 无□
	8. 有无建立电子公告服务、个人主页等栏目的信息审核、登记制度		有□ 无□
	9. 有无建立信息监视制度		有□ 无□
	10. 有无建立信息的保存、清除和备份制度		有□ 无□
	11. 有无建立病毒检测和网络安全漏洞检测制度		有□ 无□
	12. 有无建立违法案件报告和协助查处制度		有□ 无□
	13. 有无建立账号使用登记和操作权限管理制度		有□ 无□
	14. 有无落实安全管理人员岗位工作职责		有□ 无□
	15. 有无建立信息审查人员和用户的内部安全教育培训制度		有□ 无□
	16. 有无建立值班制度		有□ 无□
	17. 是否有个人主页上传信息管理制度		是□ 否□
	18. 是否有搜索引擎安全保护管理制度		是□ 否□
	19. 有无其他与安全保护相关的管理制度		是□ 否□
	20. 有无根据公安机关要求，提供有关安全管理和安全保护的技术资料和信息		有□ 无□

续表

安全技术措施	检查上网用户日志记录留存制度情况	21. 系统网络运行日志和用户使用日志记录有无保存 60 日以上	有□　无□
		22. 有无记录 IP 地址分配及使用情况	有□　无□
		23. 有无记录交互式信息发布者、主页维护者、邮箱使用者和拨号用户上网的起止时间和对应 IP 地址、交互式栏目的信息等	有□　无□
	24. 是否具有安全审计或预警功能		是□　否□
	25. 有无采取计算机防黑客入侵和病毒防护功能		有□　无□
	26. 使用何种计算机防病毒软件		
	27. 有无重要数据库和系统主要设备的冗灾备份措施		有□　无□
	28. 有无发送控制和有害信息过滤封堵技术措施		有□　无□
	29. 没有取得新闻登载资格的网站，有无登载时政、社会、文化(不包括娱乐)三类新闻		有□　无□
	30. 网站有无链接境外媒体网站和港澳台网站		有□　无□
	31. 有无建立措施配合公安机关追查有害信息的来源，协助做好取证工作		有□　无□
	32. 有无与公安机关建立二十四小时联络员工作关系		有□　无□
	33. 在紧急的情况下(包括非上班时间和节假日)，联络员是否可以按公安机关的要求及时查询资料(如 IP 等)？是否可以按公安机关的要求和指令删除有害信息		是□　否□
	34. 有无其他保护信息和系统网络安全的技术措施		有□　无□
邮件服务器安全技术保护措施	35. 是否具有邮件服务身份登记和识别确认功能		是□　否□
	36. 有无将过滤的有害信息进行整理分类，其中，有无将存在反动邮件的原始数据通过存储介质或专门的传输通道 24 小时内报送公安机关网络安全保卫部门		有□　无□
	37. 有无措施限制本地电子邮件用户一次性发送 25 封以上电子邮件		有□　无□
	38. 是否具有本地邮件服务器发送电子邮件账号核实功能，停止匿名转信服务		是□　否□
	39. 有无对邮件信头、内容和附件采取基于地址和特征字符串的过滤措施		有□　无□
	40. 缺省安装电子邮件服务软件的单位是否已关闭有关端口		是□　否□
	41. 是否安装公安机关推荐使用的反垃圾电子邮件系统		是□　否□
	42. 有无与公安机关签订有关网络与信息安全责任书，落实“谁主管，谁负责”的安全责任制度		有□　无□
安全领导小组和安全员名单及联系电话			

检查民警：　　　　　　　　　　　　　　　　　　联系电话：

被检查单位负责人：　　　　　　　　　　　　　　安全员或技术员：

3.2.4 联网单位管理

1. 管理依据

《计算机信息网络国际联网安全保护管理办法》相关规定如下：

第三条　公安部计算机管理监察机构负责计算机信息网络国际联网的安全保护管理工作。

公安机关计算机管理监察机构应当保护计算机信息网络国际联网的公共安全，维护从事国际联网业务的单位和个人的合法权益和公众利益。

第十条　互联单位、接入单位及使用计算机信息网络国际联网的法人和其他组织应当履行下列安全保护职责：

① 负责本网络的安全保护管理工作，建立健全安全保护管理制度；

② 落实安全保护技术措施，保障本网络的运行安全和信息安全；

③ 负责对本网络用户的安全教育和培训；

④ 对委托发布信息的单位和个人进行登记，并对所提供的信息内容按照本办法第五条进行审核；

⑤ 建立计算机信息网络电子公告系统的用户登记和信息管理制度；

⑥ 发现有本办法第四条、第五条、第六条、第七条所列情形之一的，应当保留有关原始记录，并在二十四小时内向当地公安机关报告；

⑦ 按照国家有关规定，删除本网络中含有本办法第五条内容的地址、目录或者关闭服务器。

第十二条　互联单位、接入单位、使用计算机信息网络国际联网的法人和其他组织(包括跨省、自治区、直辖市联网的单位和所属的分支机构)，应当自网络正式联通之日起三十日内，到所在地的省、自治区、直辖市人民政府公安机关指定的受理机关办理备案手续。

前款所列单位应当负责将接入本网络的接入单位和用户情况报当地公安机关备案，并及时报告本网络中接入单位和用户的变更情况。

第十五条　省、自治区、直辖市公安厅(局)，地(市)、县(市)公安局，应当有相应机构负责国际联网的安全保护管理工作。

第十七条　公安机关计算机管理监察机构应当督促互联单位、接入单位及有关用户建立健全安全保护管理制度。监督、检查网络安全保护管理以及技术措施的落实情况。

公安机关计算机管理监察机构在组织安全检查时，有关单位应当派人参加。公安机关计算机管理监察机构对安全检查发现的问题，应当提出改进意见，作出详细记录，存档备查。

2. 管理对象

互联网联网单位管理对象是通过接入网络与互联网连接的计算机信息网络用户，包括单位用户及个人用户。

社区、学校、图书馆、宾馆、咖啡馆、娱乐休闲中心等向特定对象提供上网服务的场所也纳入互联网联网单位管理中。

3. 管理和服务内容

(1) 督促联网单位建立信息网络安全组织机构。

(2) 督促、指导联网单位依法履行备案义务。

(3) 督促、指导联网单位建立安全管理制度。

(4) 督促、指导联网单位完善安全保护技术措施。

(5) 督促、指导联网单位定期向公安机关提交有关安全保护的信息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为。

4. 工作方法和要求

1) 全面掌握联网单位基本情况

掌握联网单位基本情况的方法包括：及时收集本行政区划内互联网运营单位(ISP、IDC)报送的联网单位情况；通过备案及时掌握联网单位的情况；通过日常管理和监控工作发现联网单位的情况。

应掌握的基本情况包括：本行政区划内联网单位的底数、服务内容、用户规模以及单位的相关情况。掌握联网单位的备案率应达到 90%。

2) 加强安全检查和指导

要求各联网单位落实安全保护管理制度和安全保护技术措施，重点检查重要网络系统的系统备份、安全审计日志记录留存以及突发性事件的应急处置措施的落实情况。具有保存 60 天以上系统运行日志和内部用户使用日志记录功能。上网日志应包括上网时间、下网时间、用户名、网卡 MAC 地址、内部 IP 地址、内部 IP 与外部 IP 地址的对应关系、访问的目标 IP 地址等信息。落实安全技术保护措施的联网单位必须达到 95%。

3) 分层次、分类型指导联网单位落实安全保护管理制度

(1) 分层次管理。

① 普通联网单位。对于用户规模在 100 个以下的联网单位，纳入普通联网单位管理，指导落实安全保护管理制度。一是依法通过正规途径接入互联网，不得私自接入，并依法履行备案义务；二是安全审计产品必须使用相应带宽的硬件产品，防止低带宽产品审计高带宽出口造成丢包。

② 大型联网单位。对于用户规模在 100～500 个之间的联网单位，纳入大型联网单位重点管理。在普通联网单位管理的基础上，还要求单位服务器必须采用专用机房统一管理。

③ 特大型联网单位。对于用户规模达到 500 个以上的联网单位，纳入特大型联网单位重点管理。在大型联网单位管理的基础上，还要求把特大型联网单位纳入互联网运营单位管理对象中，采用互联网运营单位管理模式进行管理。

(2) 分类型管理。

① 党政机关联网单位。指导建立安全保护管理制度，重点落实重要信息系统的系统备份及应急预案制度、操作权限管理制度和用户登记制度；系统重要部分的冗余或备份措施、计算机病毒防治措施以及网络攻击防范、追踪措施；对使用公网动态 IP 地址上网的用户，

上网日志应包括上网时间、下网时间、用户名、主叫电话号码、分配给用户的 IP 地址等信息。

② 宾馆旅业。指导建立安全保护管理制度,重点落实操作权限管理制度;用户登记制度、异常情况及违法犯罪案件报告和协查制度;系统运行和用户使用日志记录措施,其中对使用内部 IP 地址,通过网络地址转换技术(NAT、PAT)上网的用户,上网日志应包括上网时间、下网时间、用户名、网卡 MAC 地址、内部 IP 地址、内部 IP 与外部 IP 地址的对应关系、访问的目标 IP 地址等信息。

③ 非经营性公共上网服务场所。指导建立安全保护管理制度,重点落实操作权限管理制度、用户登记制度和备案制度,以及系统运行和用户使用日志记录保存 60 日以上措施、身份登记和识别确认措施。

④ 重点联网用户。指导建立安全保护管理制度,严格上网管理,禁止一机两用。

5. 行政处罚

(1) 根据《计算机信息网络国际联网安全保护管理办法》第二十条规定,利用国际联网制作、复制、查阅和传播有害信息或者从事危害计算机信息网络安全活动的,由公安机关给予警告,有违法所得的,没收违法所得,对个人可以并处五千元以下的罚款,对单位可以并处一万五千元以下的罚款;情节严重的,并可以给予六个月以内停止联网、停机整顿的处罚,必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格;构成违反治安管理行为的,依照治安管理处罚条例的规定处罚;构成犯罪的,依法追究刑事责任。

(2) 根据《计算机信息网络国际联网安全保护管理办法》第二十一条规定,有下列行为之一的,由公安机关责令限期改正,给予警告,有违法所得的,没收违法所得;在规定的限期内未改正的,对单位的主管负责人员和其他直接责任人员可以并处五千元以下的罚款,对单位可以并处一万五千元以下的罚款;情节严重的,并可以给予六个月以内的停止联网、停机整顿的处罚,必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格。

① 未建立安全保护管理制度的;

② 未采取安全技术保护措施的;

③ 未对网络用户进行安全教育和培训的;

④ 未提供安全保护管理所需信息、资料及数据文件,或者所提供内容不真实的;

⑤ 对委托其发布的信息内容未进行审核或者对委托单位和个人未进行登记的;

⑥ 未建立电子公告系统的用户登记和信息管理制度的;

⑦ 未按照国家有关规定,删除网络地址、目录或者关闭服务器的;

⑧ 未建立公用账号使用登记制度的;

⑨ 转借、转让用户账号的。

(3) 根据《计算机信息网络国际联网安全保护管理办法》第二十三条规定,不履行备案职责的,由公安机关给予警告或者停机整顿不超过六个月的处罚。

6. 工作流程

1) 日常管理工作流程

互联网联网单位日常管理工作流程如图 3-6 所示。

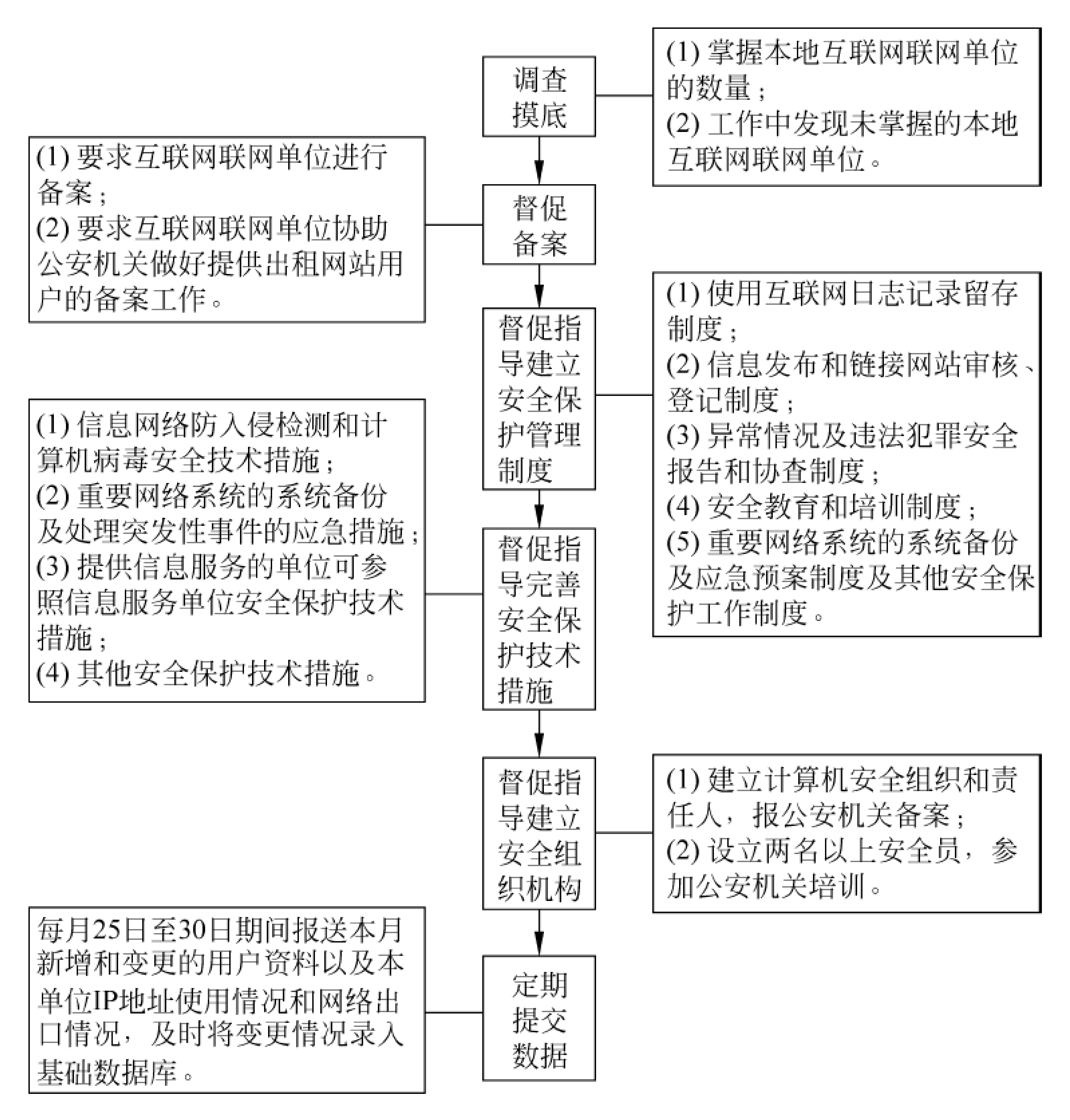


图 3-6　互联网联网单位日常管理工作流程

2）日常检查工作流程

互联网联网单位日常检查工作流程参见图 3-4 所示的互联网运营单位日常检查工作流程。

7. 相关表格

××市联网单位安全检查表

检查单位：××市公安局公共信息网络安全保卫支队　　　　　　时间：　年　月　日

<table>
<tr><td>被检查单位名称</td><td colspan="8"></td></tr>
<tr><td>单位地址</td><td></td><td colspan="2"></td><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td>法人代表</td><td></td><td colspan="2">联系电话</td><td colspan="3"></td><td colspan="2">E-mail</td></tr>
<tr><td>安全负责人</td><td></td><td colspan="2">联系电话</td><td colspan="3"></td><td colspan="2">E-mail</td></tr>
<tr><td rowspan="5">单位基本情况</td><td>行业性质</td><td colspan="2"></td><td colspan="3">服务性质</td><td colspan="2"></td></tr>
<tr><td>接入服务商</td><td></td><td colspan="2">接入方式</td><td></td><td colspan="2">介质类型</td><td></td></tr>
<tr><td>IP 地址</td><td colspan="7"></td></tr>
<tr><td>单位规模</td><td colspan="2"></td><td colspan="3">可联网信息点数</td><td colspan="2"></td></tr>
<tr><td>历史整改数</td><td colspan="2"></td><td colspan="3">完成情况</td><td colspan="2"></td></tr>
</table>

续表

<table>
<tr><td rowspan="2">安全员信息</td><td>安全员姓名</td><td></td><td>联系电话</td><td></td><td>安全员证书号码</td><td></td></tr>
<tr><td>安全员姓名</td><td></td><td>联系电话</td><td></td><td>安全员证书号码</td><td></td></tr>
<tr><td rowspan="5">安全产品信息</td><td>产品名称</td><td colspan="2"></td><td>产品类型</td><td colspan="2"></td></tr>
<tr><td>产品型号</td><td colspan="2"></td><td>应用范围</td><td colspan="2"></td></tr>
<tr><td>计算机信息系统安全专用
产品检测合格证号</td><td colspan="5"></td></tr>
<tr><td>计算机信息系统安全专用
产品销售许可证号</td><td colspan="5"></td></tr>
<tr><td>安装时间</td><td colspan="2"></td><td>安装单位</td><td colspan="2"></td></tr>
<tr><td rowspan="13">落实安全保护管理制度情况</td><td colspan="5">有无建立网络安全领导小组、确立小组负责人</td><td>有□　无□</td></tr>
<tr><td colspan="5">有无落实组长、小组人员岗位工作职责</td><td>有□　无□</td></tr>
<tr><td colspan="5">有无建立计算机机房安全管理制度</td><td>有□　无□</td></tr>
<tr><td colspan="5">有无建立用户登记制度和操作权限管理制度</td><td>有□　无□</td></tr>
<tr><td colspan="5">有无建立网络安全漏洞检测和系统升级管理制度</td><td>有□　无□</td></tr>
<tr><td colspan="5">有无建立电子公告系统用户登记制度</td><td>有□　无□</td></tr>
<tr><td colspan="5">有无建立交互栏目 24 小时巡查制度</td><td>有□　无□</td></tr>
<tr><td colspan="5">有无建立信息发布审核、登记、保存、清除和备份制度，信息群发服务管理制度</td><td>有□　无□</td></tr>
<tr><td colspan="5">有无制定网络安全事故处置措施</td><td>有□　无□</td></tr>
<tr><td colspan="5">有无配备 2～4 名计算机安全员，须持证上岗</td><td>有□　无□</td></tr>
<tr><td colspan="5">有无建立安全教育培训制度</td><td>有□　无□</td></tr>
<tr><td colspan="5">有无落实备案制度</td><td>有□　无□</td></tr>
<tr><td colspan="5">有无建立违法案件报告和协助查处制度</td><td>有□　无□</td></tr>
<tr><td rowspan="8">落实安全保护技术措施情况</td><td colspan="5">有无建立包括 IP 地址分配及使用情况，交互式信息发布者、主页维护者、邮箱使用者和拨号用户上网的起止时间和对应 IP 地址，交互式栏目信息等内容的系统网络运行日志和用户使用日志记录功能。</td><td>有□　无□</td></tr>
<tr><td colspan="5">有无建立安全审计及预警措施</td><td>有□　无□</td></tr>
<tr><td colspan="5">有无建立网络攻击防范、追踪措施</td><td>有□　无□</td></tr>
<tr><td colspan="5">有无建立计算机病毒防治措施</td><td>有□　无□</td></tr>
<tr><td colspan="5">有无建立身份登记和识别确认措施</td><td>有□　无□</td></tr>
<tr><td colspan="5">有无系统运行和用户使用日志记录</td><td>有□　无□</td></tr>
<tr><td colspan="5">系统网络运行日志和用户使用日志记录有无保存 60 日以上</td><td>有□　无□</td></tr>
<tr><td colspan="5">有无记录发生案件、事故和发现计算机有害数据的情况</td><td>有□　无□</td></tr>
<tr><td rowspan="4">安全保护技术措施检测情况</td><td colspan="5">产品运行情况</td><td></td></tr>
<tr><td colspan="5">有无日志记录信息</td><td>有□　无□</td></tr>
<tr><td colspan="5">日志记录是否完整</td><td>是□　否□</td></tr>
<tr><td colspan="5">日志格式是否规范</td><td>是□　否□</td></tr>
<tr><td>检查意见</td><td colspan="6"></td></tr>
</table>

检查民警：　　　　　　　　　　　　　　　　被检查单位负责人：

3.3　计算机病毒等破坏性程序防治管理

1994 年 2 月 18 日《中华人民共和国计算机信息系统安全保护条例》第二十八条给计算机病毒所下的定义是："计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。"

计算机病毒具有隐蔽性强、潜伏期长、传播范围大、危害结果严重等特点，是计算机安全的头号杀手。其实，计算机病毒只是破坏性程序的一种主要表现形式，破坏性程序还包括"设备炸弹"、"逻辑炸弹"、"野兔"、"特洛伊木马"、"蠕虫"等其他多种形式。

计算机病毒传播的途径主要集中在通过网页下载，其次是电子邮件，再次是局域网，而通过光盘或者磁盘感染的比例最低。目前，计算机病毒越来越多是以窃取银行账号、信息卡密码、游戏账号、邮箱账号、机密文件等偷窃个人或企事业核心信息为主要目的。

3.3.1　管理依据

1.《中华人民共和国计算机信息系统安全保护条例》(国务院令 147 号，1994 年 2 月 18 日)

第十五条　对计算机病毒和危害社会公共安全的其他有害数据的防治研究工作，由公安部归口管理。

2.《计算机病毒防治管理办法》(公安部第 51 号令，2000 年 4 月 26 日)

第四条　公安部公共信息网络安全监察部门主管全国的计算机病毒防治管理工作。

地方各级公安机关具体负责本行政区域内的计算机病毒防治管理工作。

3.3.2　管理对象

(1) 制作、传播计算机病毒的行为。

(2) 发布虚假的计算机病毒疫情的行为。

(3) 从事计算机病毒防治产品生产的单位。

(4) 从事计算机设备或者媒体生产、销售、出租、维修行业的单位和个人。

《计算机病毒防治管理办法》中第二十一条规定了关于计算机病毒疫情的定义，是指某种计算机病毒爆发、流行的时间、范围、破坏特点、破坏后果等情况的报告或者预报。

3.3.3　管理职责

(1) 监督、检查、指导信息系统运营、使用单位建立、落实下列计算机病毒等破坏性程序防治管理制度和安全保护技术措施：

① 制定计算机病毒防治管理制度和技术规程。

② 采取计算机病毒安全技术防治措施。

③ 对计算机信息系统应用和使用人员进行计算机病毒防治教育和培训。

④ 建设计算机病毒防治系统,通过控制信息的出入口,防止病毒入侵,并对已经入侵的病毒及时进行检测和清除,并做好检测、清除的记录。

⑤ 购置和使用具有计算机信息系统安全专用产品销售许可证的计算机病毒防治产品。

⑥ 对因计算机病毒引起的计算机信息系统瘫痪、程序和数据严重破坏等重大事故及时向公安机关报告,并保护现场。

⑦ 向公安机关报告发现的计算机病毒,并协助公安机关追查计算机病毒的来源。

(2) 督促从事计算机设备或者媒体生产、销售、出租、维修行业的单位及个人做好计算机设备或者媒体的病毒检测、清除工作。

(3) 开展本地计算机病毒疫情调查,并举办各种计算机病毒等破坏性程序防范的宣传活动。

(4) 只有取得从事计算机病毒防治产品生产资格的单位才能允许存储计算机病毒,并且要到公安机关网络安全保卫部门进行审批、备案;

(5) 督促计算机病毒防治产品研制、生产、销售单位,安全服务机构和用户对发现的计算机病毒提取样本,报送公安机关网络安全保卫部门。

(6) 建设大型的网络安全监控系统。在骨干网、支网、用户网等不同层次上建设网络安全监控系统,实时检测网络病毒传播情况,及时发现新病毒预警,及时发现病毒源。

(7) 将接收的计算机病毒样本上报上级公安机关网络安全保卫部门。

(8) 指导、组织社会技术支撑力量对发现的计算机病毒及时进行处置,对用户级的计算机病毒控制与处置工作提供技术支持。包括提取计算机病毒样本,交付指定计算机病毒防治机构进行解剖、分析后,形成计算机病毒疫情分析报告和解决方案。

(9) 加强对计算机病毒防治产品的监管。任何单位和个人销售、附赠的计算机病毒防治产品,应当具有计算机信息系统安全专用产品销售许可证,并贴有“销售许可”标记。

(10) 利用行政管理手段,严格控制病毒传播源,严厉处罚各类病毒传播行为和传播人。

3.3.4 工作要求

(1) 全面掌握病毒信息,建立病毒预警机制。一是及时收集本行政区划计算机病毒研究机构和各种社会技术支撑力量报送的情况,及时掌握计算机病毒信息;二是通过备案及时掌握相关服务单位的情况;三是通过日常管理和监控工作发现计算机病毒信息;四是通过上级有关部门和各地网络安全保卫部门的通报,掌握计算机病毒信息;五是通过技术措施发现计算机病毒信息。

(2) 建立病毒快速反应机制。通过各种渠道及时发现新爆发的严重计算机病毒疫情,积极组织计算机病毒防治机构进行解剖、分析,出具计算机病毒疫情分析报告和解决方案;同时,通过新闻媒体发布计算机病毒疫情信息,通知社会各界做好防治工作。

(3) 加强计算机病毒防治知识宣传、教育和培训。一是每半年举行一次计算机病毒等破坏性程序防范的宣传活动；二是在本地政府网站上设立计算机病毒防治专栏；三是对信息系统运营、使用单位的安全员定期组织计算机病毒防治技术培训；四是开设计算机病毒报警电话，接受群众报警和咨询。

(4) 全面掌握计算机病毒防治产品研发机构的情况。重点掌握研发机构基本情况、服务内容和生产产品情况，督促研发机构就其本身及所生产销售的产品依法履行备案义务，指导其将计算机病毒防治产品送公安机关进行检测。

3.3.5　行政处罚

1.《刑法》规定

第二百八十六条　违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役，后果特别严重的，处五年以上有期徒刑。违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

2.《中华人民共和国治安管理处罚法》规定

第二十九条　有下列行为之一的，处五日以下拘留；情节较重的，处五日以上十日以下拘留：

(1) 违反国家规定，侵入计算机信息系统，造成危害的；

(2) 违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行的；

(3) 违反国家规定，对计算机信息系统中存储、处理、传输的数据和应用程序进行删除、修改、增加的；

(4) 故意制作、传播计算机病毒等破坏性程序，影响计算机信息系统正常运行的。

3.《中华人民共和国计算机信息系统安全保护条例》规定

第二十三条　故意输入计算机病毒以及其他有害数据危害计算机信息系统安全的，或者未经许可出售计算机信息系统安全专用产品的，由公安机关处以警告或者对个人处以五千元以下的罚款、对单位处以一万五千元以下的罚款；有违法所得的，除予以没收外，可以处以违法所得 1 至 3 倍的罚款。

4.《计算机信息网络国际联网安全保护管理办法》规定

第六条　任何单位和个人不得从事下列危害计算机信息网络安全的活动：

(1) 未经允许，进入计算机信息网络或者使用计算机信息网络资源的；

(2) 未经允许，对计算机信息网络功能进行删除、修改或者增加的；

(3) 未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、

修改或者增加的；

(4) 故意制作、传播计算机病毒等破坏性程序的；

(5) 其他危害计算机信息网络安全的。

第二十条　违反法律、行政法规，有本办法第五条、第六条所列行为之一的，由公安机关给予警告，有违法所得的，没收违法所得，对个人可以并处五千元以下的罚款，对单位可以并处一万五千元以下的罚款；情节严重的，并可以给予六个月以内停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格；构成违反治安管理行为的，依照治安管理处罚条例的规定处罚；构成犯罪的，依法追究刑事责任。

5.《计算机病毒防治管理办法》规定

(1) 在非经营活动中有违反下列行为之一的，由公安机关处以一千元以下罚款；在经营活动中有违反下列行为之一，没有违法所得的，由公安机关对单位处以一万元以下罚款，对个人处以五千元以下罚款；有违法所得的，处以违法所得三倍以下罚款，但是最高不得超过三万元。

① 任何单位和个人不得制作计算机病毒；

② 向他人提供含有计算机病毒的文件、软件、媒体；

③ 销售、出租、附赠含有计算机病毒的媒体；

④ 其他传播计算机病毒的行为。

(2) 违反下列行为之一的，由公安机关对单位处以一千元以下罚款，对单位直接负责的主管人员和直接责任人员处以五百元以下罚款；对个人处以五百元以下罚款。

① 任何单位和个人不得向社会发布虚假的计算机病毒疫情；

② 从事计算机病毒防治产品生产的单位，应当及时向公安部公共信息网络安全监察部门批准的计算机病毒防治产品检测机构提交病毒样本。

(3) 计算机病毒防治产品检测机构应当对提交的病毒样本及时进行分析、确认，并将确认结果上报公安部公共信息网络安全监察部门。违反此规定的，由公安机关处以警告，并责令其限期改正；逾期不改正的，取消其计算机病毒防治产品检测机构的检测资格。

(4) 计算机信息系统的使用单位有下列行为之一的，由公安机关处以警告，并根据情况责令其限期改正；逾期不改正的，对单位处以一千元以下罚款，对单位直接负责的主管人员和直接责任人员处以五百元以下罚款：

① 未建立本单位计算机病毒防治管理制度的；

② 未采取计算机病毒安全技术防治措施的；

③ 未对本单位计算机信息系统使用人员进行计算机病毒防治教育和培训的；

④ 未及时检测、清除计算机信息系统中的计算机病毒，对计算机信息系统造成危害的；

⑤ 未使用具有计算机信息系统安全专用产品销售许可证的计算机病毒防治产品，对计算机信息系统造成危害的。

(5) 从事计算机设备或者媒体生产、销售、出租、维修行业的单位和个人，应当对计算机

设备或者媒体进行计算机病毒检测、清除工作,并备有检测、清除的记录。违反此规定的,没有违法所得的,由公安机关对单位处以一万元以下罚款,对个人处以五千元以下罚款;有违法所得的,处以违法所得三倍以下罚款,但是最高不得超过三万元。

3.4　计算机安全员培训及管理

1999 年 4 月,公安部、人事部发出《关于开展计算机安全员培训工作的通知》,对培训对象、培训内容、培训方式步骤、培训考试、培训工作的组织和管理都做了明确规定;2006 年 5 月,公安部办公厅、人事部办公厅联合发布《关于开展信息网络安全专业技术人员继续教育工作的通知》,将信息网络安全专业技术人员继续教育工作作为一项长期工作,纳入公安机关信息网络安全监督管理工作之中,逐步建立一支与公安机关密切配合、维护信息网络安全的社会力量。

3.4.1　培训目的

培训计算机安全员的目的,在于提高相关知识水平,从而提高各单位自身的网络安全防范能力,防范和制止计算机犯罪、安全事故的发生。同时通过培训和日常的沟通联络,组建一支以计算机安全员为主的社会辅助力量,协助公安机关网络安全保卫部门开展网上重大突发事件的应急处置工作以及信息网络安全的群防群治工作。

3.4.2　培训对象

计算机安全员培训对象包括:

(1) 负责计算机安全监察工作的各级公安机关民警和保卫部门的保卫干部。

(2) 计算机信息系统使用单位安全管理责任人、信息审查员。

(3) 重点安全保护单位计算机信息系统维护和管理人员。

(4) 计算机信息网络国际联网的互联单位和接入单位的有关人员。

(5) 安全服务机构专业技术人员、安全服务管理人员。

(6) 互联网上网服务营业场所的安全管理人员、经营管理人员、专业技术人员。

(7) 从事计算机安全工程和安全产品开发、生产单位的技术人员。

3.4.3　培训内容

计算机安全员培训内容有:

(1) 计算机网络安全:网络的基本安全对策,常见的网络信息安全问题,网络安全隐患,信息系统安全风险管理的方法,计算机信息系统安全事故的查处和管理,计算机犯罪的防范、打击和案件报告制度等其他计算机安全保护的相关内容。

(2) 计算机病毒及防治:常见的计算机病毒及黑客程序的检测、清除和防范。

(3) 计算机安全专用产品销售许可管理制度。

(4) 计算机信息系统安全保护法律、法规。

3.4.4 培训方式及要求

计算机安全员培训原则上采取脱产培训方式，培训时间不少于40学时，使用全国统编教材和统编大纲。

培训机构需经过省级以上公安机关考核、审查和资格认证，培训教员要持证上岗。同时，培训机构要具备社会办学许可证照，具有较强网络安全师资力量，要到所在地地级以上(含地级)公安机关网络安全保卫部门备案。

学员培训后参加由公安、人事部门联合组织的统一考试。考试合格者，由公安、人事部门认定其计算机安全员培训合格，并在合格证明材料上加盖省、自治区、直辖市计算机安全员培训考试专用章。党政机关、金融财税系统、国家重要经济部门等重要领域的计算机安全管理人员、工程技术人员和重要岗位上的计算机技术人员、操作人员必须持证上岗。凡未取得考试合格证者，不得从事相关工作。

3.4.5 计算机安全员的管理

培训机构对取得计算机安全员合格证书的培训人员的相关资料建档管理，并定期报送公安机关网络安全保卫部门。合格证书有效期满后，应由培训机构对持证人重新进行资格培训。

计算机安全员应履行的职责包括：

(1) 依据国家有关法规政策，从事本单位的信息网络安全保护工作，确保网络安全运行。

(2) 执行本单位计算机信息网络安全管理的各项规章制度。

(3) 在公安机关网络安全保卫部门的监督、指导下进行信息网络安全检查和安全宣传工作。

(4) 向公安机关及时报告发生在本单位网上的有害信息、安全事故和违法犯罪案件，并协助公安机关做好现场保护和技术取证工作，配合公安机关开展案件调查工作。

(5) 发现有关危害信息网络安全的计算机病毒、黑客等方面的情报应及时向公安机关报告。

(6) 应保持与公安机关联系渠道的畅通，保证各项信息网络安全政策、法规在本单位的落实，积极接受公安机关网络安全保卫部门的业务监督检查。

(7) 在发生网络重大突发性事件时，应随时响应，接受公安机关网络安全保卫部门调遣，承担处置任务。

(8) 向本单位的负责人提出改进计算机信息网络安全工作的意见和建议。

(9) 与信息网络安全保护有关的其他工作。

各单位网络安全组织的安全责任人及安全技术人员应切实履行各项安全职责，对不依法履行职责，造成安全事故和重大损害的，由公安机关予以警告，并建议其所在单位给予纪律或经济处理，情节严重的，依法追究其刑事责任。

习　题

1. 如何正确理解信息网络安全监督管理的指导思想？
2. 信息网络安全监督管理工作的主要任务是什么？
3. 公安机关网络安全保卫部门的备案对象包括哪些？
4. 互联网单位包括哪些？它们都有哪些具体的管理内容？
5. 违反计算机病毒等破坏性程序防治管理的行政处罚有哪些？
6. 计算机安全员培训的内容是什么？

第4章

互联网信息内容安全管理

【内容提要】

本章主要介绍互联网信息内容安全管理的法律规定、管理机构及管理的责任、制度和措施要求；通过本章的学习，掌握对互联网有害信息的认定以及互联网信息内容安全管理方面的有关规定。

4.1 互联网信息内容安全管理概述

互联网传播具有信息量大、易检索、便捷快速等独特优势，在某种意义上说，互联网已经成为继报纸、广播、电视后的又一新的传播媒介——第四媒体。与此同时，以移动技术为主导的第五媒体——手机网络与互联网络的融合趋势日益明显，网络淫秽色情及低俗信息传播渠道多样多变，互联网传播信息内容的安全对国家安全、经济发展、社会秩序等的影响愈发巨大。因此，整治互联网和手机媒体淫秽色情及低俗信息，有效切断淫秽色情和低俗网站的利益链条，依法加强互联网信息内容的基础管理，成为信息网络安全管理中需要认真对待的最为严肃的内容之一。

4.1.1 互联网信息内容安全管理基本概念

互联网信息内容的安全管理是互联网信息传播时代非常重要和重视的一项工作。互联网信息内容安全的主要含义是指作为大众传播信息工具的互联网上所传播的信息内容符合国家法规的规定，并且合乎普遍认可的社会道德伦理。

互联网信息内容安全管理是指以政府、企业和社会各方面为主体，共同参与对互联网上传播信息内容的控制和制约，禁止有害信息的传播，从而使互联网上的信息内容完整、无害、有序地进行传播。

从广泛意义上来说，互联网信息内容安全要控制的信息内容包括：E-mail中携带的病毒、恶意代码以及秘密信息；浏览的Web页的合法性——是否为病毒、恶意代码和色情信息等；下载信息的合法性；垃圾邮件；非法攻击国家、有碍和平的信息等。对于互联网内容的管理，不同国家有不同的标准。在我国，可以用合法、合情、合理来概括管理的标准。首先，不能违反国家法律，即违反我国宪法和法律的言论不容许在网上泛滥；其次，要合情、合

理，合乎中国社会通常公认的伦理道德和人情。

4.1.2　国外互联网信息内容安全管理现状

互联网是一个开放的世界，但“没有规矩，不成方圆”，虚拟的互联网也并非完全的自由地带。网络犯罪有恃无恐、网络谣言蛊惑人心、网络色情泛滥成灾、网络欺诈层出不穷……很多现实案例已经表明，互联网上一旦出现法律和监管上的真空，国家安全、信息安全、电子商务、个人隐私、未成年保护等合法行为、合法权益、合理诉求必将遭受冲击和破坏。依法管理互联网已成国际惯例，只有明确互联网法律保护什么，禁止什么，明确互联网主体参与者的权利和义务，才能保障互联网健康、有序、快速的发展；只有让法律法规适应日新月异的互联网技术发展，依法管理好互联网，才能让网民安全使用互联网，共享互联网科技进步带来的硕大成果。

1. 美国

美国是互联网发展最早、普及率最高的国家，3 亿多人口中就有接近 2.5 亿网民，普及率居世界首位。同时，美国有着当今世界最成熟和最有效率的互联网监控和管制措施，为互联网行业的发展创造了较良好的环境，进而推动互联网行业的迅速发展。

整体而言，美国在互联网的管理上规章制度基本健全。联邦政府和各州地方政府通过立法，不论是战略层面还是策略层面，不论是技术层面还是管理层面，都对网络实施有效监管。美国主管互联网的职能主管部门是“联邦通讯委员会”，它负责互联网传播的规范和引导工作，主要从以下三个方面对互联网进行监管。

(1) 依法执行监管

为有效地管理互联网，自 1978 年以来，美国国会及政府各部门先后通过了 130 项相关的法律和法规。同时，美国各州均制定了有关互联网管理的地方法规和处罚办法。

(2) 重视行业自律

在制定有关互联网管理法律、法规的同时，美国政府鼓励互联网行业加强自律。各种专业协会通过行业规范、公约等共同认可的条文推动行业实施自律，以确保行业行为符合法律规定和道德要求，也避免在政府管制中处于被动。

(3) 鼓励公众参与

鼓励公众参与对互联网的监督也是美国政府采取的一项重要的网络监管措施。美国不少非政府组织主动地参与对互联网的监管活动，尤其是针对互联网上出现的儿童色情内容。美国“联邦通讯委员会”在 1999 年专门成立了一个执行局，负责接待公众的举报和投诉。公众可以通过信件、电子邮件、传真等多种方式进行投诉举报。

2. 英国

在互联网上各种有害信息层出不穷的形势下，英国政府一方面采取各种措施强化网民自律意识和网络运营商的社会责任意识；另一方面通过立法来保证网络世界安全、健康地运转。2009 年，英国使用互联网的家庭占全国家庭总数的 70%，成人用户占全国成人总数的 76%。

因为网络日益重要且内容良莠不齐,英国较早着手互联网的管理,形成了一套独具特色、各方较为满意的监管方法,倡导行业自律和协调,监督而非监控,是英国网络监管的重要特点。

作为英国互联网的主要监管机构,“互联网监察基金会”以《R3 安全网络协议》为基础,确立了两个基本的管理指导思想:对其他媒介适用的法律,对互联网同样适用。世界任何地方的儿童色情、在英国国内的犯罪内容和煽动种族仇恨都是互联网上的“非法内容”;对不违法,但可能引起用户反感的内容进行分级和标注,由用户自愿选择接受还是拒绝。“互联网监察基金会”的管理方法主要有以下三方面:

(1) 建立热线,接待公众举报和投诉。

(2) 建立非法内容“统一资源定位符”(URL)名单,以便网络企业自己决定是否关闭有关链接。

(3) 对于不违法,但可能引起用户反感的网络内容,网络管理者应分级和标注,以便用户自行选择取舍。

3. 法国

法国政府对互联网的作用始终以积极的态度进行普及推广,同时又以严格的法律对其进行管理。早在 2006 年,法国即通过了《信息社会法案》,旨在加强对互联网的“共同调控”,在给人们提供自由空间和人权自由的同时,充分保护网民的隐私权、著作权以及国家和个人的安全。2009 年 4 月,法国国民议会与参院又通过了被认为是“世界上最为严厉的”打击网络非法下载行为的法案,并据此成立了“网络著作传播与权利保护高级公署”,维护公共秩序,保护著作权人的合法权益,打击侵权盗版活动。

法国互联网管理的另一特点是十分重视对未成年人的保护。法国教育部还以控制加引导的方式,一方面打击网络犯罪,同时利用网络开展文明教育,引导学生在上网时提高警惕,防止黄色及不良内容的侵害。此外,学校还在这方面发挥了积极的作用,以学生为对象,积极进行网上文明教育。在校园网上安装浏览自动监视器,限制学生的上网内容及范围。一些非政府组织也积极加入保护青少年免受“网毒”危害的队伍,形成了一个从政府、学校到社会的监督保护网络,大大降低了互联网这把“双刃剑”对青少年的伤害程度。

4. 德国

严谨认真的德国人对互联网内容管理可以说是宽容有度。各项法律的实施,既体现了网络言论的自由性,又根据国家和社会发展要求对其给以严格的限制。在合法性原则的前提下,德国建立了措施严厉的执法队伍,保证法制的落实,规范互联网内容管理。管理方法主要有以下三方面:

(1) 信息控制:自由与规制并举

作为德国宪政体系基础的《基本法》明确强调,“每个人都有表达和传播观点的权力,通过书面或视频方式,人们可以合法获得信息,不受任何阻碍”,德国“不进行事前审查”。在网络服务方面,针对数字化传媒制定的《多媒体法》指出,“任何人可以自由从事网络传播和经营,不受限制”。但是法律也规定“所有权力都要受到一般法律的限制”。德国对互联网信息

传播自由所采取的保障方式是相对的，以便在“个人利益”与“公众利益”之间求得平衡。当两者发生冲突的时候，管理上会更多考虑到国家利益和公众利益，个人言论自由价值一方需要做出退让。因此，德国对个人可能发出的具有危害性的网络言论进行的监管，既阻止了通过网络手段危害社会的行为，又确保了公民一如既往地拥有言论自由和通信自由的权利。

(2) 防范重点：保护未成年人免受侵害

保护未成年人免受互联网上不良信息的危害，是德国网络信息管理的重中之重。德国联邦政府为此建立了“危害青少年媒体检查处”，专门负责识别和检查互联网信息内容，监测不良信息网站的发展状况，将有害信息记录在案，并随时运用技术手段确保未成年人无法接触和翻阅这些内容，保证媒体传播信息的安全性。“危害青少年媒体检查处”还与一些商业机构合作，免费为青少年提供过滤器等技术软件，通过技术手段防范不良信息的影响。

(3) 严格执法：加强内容监管力度

德国是发达国家中第一个对互联网不良言论进行专门立法监管的国家，他们对有害言论的法律制裁和行政处罚措施非常严格。

德国联邦内政部是负责互联网信息安全的最高国家机构，重点防范有害信息及言论的传播；德国依法设立了网络警察，负责监控有害信息的传播，一旦发现登有违法言论和图片的网站，立即查封。德国刑事司法机关还不断查找网上极端主义、恐怖主义活动内容及其传播者踪迹。他们还与美国联邦调查局、欧洲刑警组织等机构开展国际合作，加强打击网络犯罪力度，共同监管互联网信息传播。

5. 日本

作为一个经济发达、计算机和互联网高度普及的国家，层出不穷、络绎不绝的网上犯罪一直困扰着日本政府和普通民众。日本政府与网络运营商协调一致，根据内紧外松的原则，主要通过法律手段不断加强对互联网的监管。

早在1984年，日本制定了管理互联网的《电讯事业法》。进入21世纪之后，随着互联网技术的发达和网络的普及，日本相继制定了《规范互联网服务商责任法》和《打击利用交友网站引诱未成年人法》、《青少年安全上网环境整备法》和《规范电子邮件法》等法律法规，有效遏制了网上犯罪和违法、有害信息。2011年，日本内阁会议决定向国会提交部分修改刑法的草案，草案内容不仅将制作、传播、拥有计算机病毒纳入刑法处罚的范围，而且还规定政府可以要求网络运营商保存某特定用户最长60天的上网履历和通信记录。此次修改刑法，一方面是为了加重对制作和传播计算机病毒的处罚力度，另一方面也为今后在侦破网络犯罪时，从网络运营商那里获取用户的上网信息提供了法律依据。

日本对于互联网的管理除了依据刑法和民法之外，还制定了《个人信息保护法》、《反垃圾邮件法》、《禁止非法读取信息法》和《电子契约法》等专门法规来处置网络违法行为。网络服务提供商ISP和网络内容提供商ICP、网站、个人网页、网站电子公告服务，都属于法律规范的范畴。信息发送者通过互联网站发送违法和不良信息，登载该信息的网站也要承担连带民事法律责任，网站有义务对违法和不良信息进行监管。

6. 韩国

韩国是公认的世界上互联网最发达、普及率最高的国家之一，也是世界上首个强制实行网络实名制的国家。从2007年开始，韩国制定了非常严格的网络个人认证制度，对主要的网站强制实行个人认证制度，就是指在用户登录时需要对姓名和身份证号码进行确认，以使该用户在网上发布信息时怀有更强的责任感。经过多年的发展和完善，韩国目前已通过立法、监督、管理和教育等措施，对邮箱、论坛、博客，甚至网络视频和游戏网站等实行了实名制管理。

实名制不仅在减少网络虚假信息传播、恶意留言，以及由此引发的网络暴力等方面作用明显，也为韩国政府治理“网络中毒”等社会问题提供了技术保障。针对日益严重的青少年“网络中毒”问题，韩国政府对各大游戏网站引入实名制进行管理。2010年4月，韩国文化体育观光部推出了一系列措施，旨在预防及消除青少年沉溺网络游戏成瘾。由于实行实名制，系统能够轻易识别出游戏中的未成年人。对那些不符合规定的未成年玩家，一旦超过规定的游戏时间，系统将采取减慢游戏速度、自动断开链接等强制措施。

实名制自实施以来，在净化网络环境，维护网络安全等方面发挥了重要作用。不过，韩国政府表示，韩国实行网络实名制的最大意义，在于树立网民的责任和自律意识，而自律才是网络管理的核心。

7. 新加坡

新加坡是世界上在网络管理方面最为成功的国家之一。新加坡从立法、执法、准入以及公民自我约束等渠道加强网络管理，在确保国家安全及社会稳定的前提下，最大限度地保障网民的网络遨游权利。新加坡早在1981年就开始制订一系列的计算机化与信息科技策略——全国计算机化蓝图，随后又出台全国信息科技蓝图、全联新加坡计划和IN2015蓝图，并投入巨资打造“智慧岛”。新加坡对网络实行统一管理，但在严格监管的同时也有务实和灵活的一面，目的是促进网络健康发展，以服务于国家和社会。

首先，新加坡政府高度重视互联网的立法及执法工作，将国家安全及公共利益置于首位。政府将《国内安全法》、《煽动法》、《广播法》以及《互联网实务法则》等相关法律有机结合起来，严厉打击和制止任何个人、团体或国家利用网络来危害国家安全的行为。

其次，严格控制网站的创立及网络服务内容。新加坡政府规定，互联网内容提供商有义务协助政府删除或屏蔽任何被认为是危害公共道德、公共秩序、公共安全和国家和谐等内容及网站，如不履行义务，互联网内容提供商将被处以罚款，或者暂停营业执照。政府还鼓励互联网内容提供商开发推广网络管理软件，协助用户过滤掉不适宜的内容。

此外，加强公共教育，提高公民自觉过滤意识。新加坡政府认为，有效管理互联网的长远之计在于加强公共教育，政府鼓励供应商开发推广“家庭上网系统”，帮助用户过滤掉不合适的内容。新加坡政府1999年成立“互联网家长顾问组”，由政府出资举办培训班，帮助家长指导孩子安全上网。从2003年1月起，传媒发展局还设立了500万美元的互联网公共教育基金，用于研制开发有效的内容管理工具、开展公共教育活动和鼓励安装绿色上

网软件。

4.1.3　我国互联网信息内容安全管理基本原则

互联网信息内容管理的基本原则必须符合我国社会经济规律及互联网业务运行规律，符合互联网信息内容管理的根本价值和最终目的，真实、全面、集中地反映国家法律调整和制约下的互联网信息内容安全管理关系的客观要求。我国在互联网信息内容安全管理方面的基本原则主要包括以下三个方面。

1. 主体责任原则

主体责任原则，即"谁运营谁负责"的原则，其运营的主体包括互联网接入服务单位(ISP)和互联网信息服务单位(ICP)。实践中，我国互联网接入服务单位(ISP)、互联网信息服务单位(ICP)往往会与公安机关签订有关网络与信息安全责任书，落实"谁运营谁负责"的安全责任制度。

贯彻"谁运营谁负责"的安全责任制度，还必须对互联网接入服务单位(ISP)和互联网信息服务单位(ICP)进行相应的互联网安全培训，包括互联网信息安全、运行安全、实体安全、法规教育等，提高互联网安全意识。

2. 行政监管原则

行政监管原则，是指行政机关运用行政手段或准立法、准司法手段对互联网信息内容的控制，是以一定规则、方法或确立的模式对特定主体的特定行为或特定内容通过主管、检查、监察督促，以实现对其的监管、确定或控制。通过政府机构对互联网信息内容安全的行政监管，可以克服过度市场竞争带来的负面影响，保护网络用户的合法权益，防止淫秽色情、迷信暴力等趣味低下的不良信息大行其道；同时可以利用法律行政等强制力，实施强有力的监管，以解决技术手段和行业自律无法解决的问题，确保国家在网络空间中的根本利益。

互联网信息内容安全行政监管的对象主要有：政府机构、通信运营机构、互联网接入服务单位(ISP)、互联网信息服务单位(ICP)、家庭用户及商业企业用户、安全服务提供者等。

3. 行业自律原则

依靠有限的政府机构很难在技术、人力、资源上承担巨大的互联网信息安全监管工作。有必要充分利用各种社会组织，如互联网络组织、技术联盟、行业协会等的影响和号召力，协助政府甚至直接承担一定的网络安全监管职能，发挥其自治规范的作用。自律组织可通过其灵活地制定、修正自律规则来补救网络安全监管法律滞后的缺陷。

同时，行业组织及其自律性监管还可在一定程度上起到约束政府监管主体滥用权力的作用。权力的过度集中会促使权力的滥用和腐败，因此，培育监管主体的多元化，尤其是辅助性的监管主体非常必要。

4.2 互联网信息内容安全管理体系

4.2.1 互联网信息内容安全管理机构及职责

我国政府高度重视互联网信息内容安全管理工作。2009 年 1 月 21 日，国务院新闻办、工业和信息化部、公安部、文化部、工商总局、广电总局、新闻出版总署等七部委召开联席会议，进一步部署整治互联网低俗之风专项工作，坚持不懈地搞好整治互联网和手机媒体淫秽色情及低俗信息的行动。

实际上，没有任何组织、企业或政府能够拥有 Internet，它是由一些独立的管理机构管理的，每个机构都有自己特定的职责。我国《互联网信息服务管理办法》第 18 条规定："国务院信息产业主管部门和省、自治区、直辖市电信管理机构，依法对互联网信息服务实施监督管理。新闻、出版、教育、卫生、药品监督管理、工商行政管理和公安、国家安全等有关主管部门，在各自职责范围内依法对互联网信息内容实施监督管理。"针对多部门共管互联网的现状，必须建立健全统一协调、职责明确、运转有效的监管体制。同时，权力与职责统一是法治条件下建立权力正常行使和维护相对人权益之间平衡的关键。

1. 公安机关

对互联网信息内容的安全监管工作是公安机关的一项法定职责，是指公安机关网络安全保卫部门运用行政手段，依法监督、检查、维护网上公共秩序，保证互联网上传播信息内容的安全。

1994 年 2 月 18 日国务院发布了《中华人民共和国计算机信息系统安全保护条例》，明确规定由公安部主管全国计算机信息系统安全保护工作。

1995 年 2 月 28 日第八届全国人民代表大会常务委员会第十二次会议通过的《中华人民共和国人民警察法》，明确规定公安机关的人民警察具有监督管理计算机信息系统的安全保护工作职责。

1997 年 12 月 16 日公安部发布了《计算机信息网络国际联网安全保护管理办法》，将公安机关的监督职权扩展到了信息网络的国际联网领域，同时规定了"谁主管谁负责"原则。

2000 年 12 月 28 日第九届全国人民代表大会常务委员会第十九次会议通过的《全国人民代表大会常务委员会关于维护互联网安全的决定》，进一步明确了各部门和公安机关在维护互联网安全方面的职权和责任。

2. 通信管理部门

通信管理部门的监管职权具体包括：依法对互联网信息服务实行监督管理；为从事经营性互联网信息服务的单位办理互联网信息增值电信业务经营许可证；为从事非经营性互联网信息服务单位办理备案手续；依法监督和管理互联网电子公告服务；对互联网接入服

务商、互联网信息服务提供者和联网单位的联网备案、记录留存、有害信息报告、清除等安全管理制度的落实情况进行监督检查；对违规从事网上业务的境内网站，依法采取责令整顿、予以关闭等行政处罚措施。

实践中，我国信息产业部和各地通信管理局也在认真履行其监管职责。如根据全国开展打击淫秽色情网站专项行动电视电话会议的部署，2004 年 7 月 19 日信息产业部成立了专项行动领导小组，制定并印发了《信息产业部打击淫秽色情网站专项行动工作方案》，要求各地通信管理局和各相关电信运营企业结合各地实际情况和各自特点，做好贯彻落实工作，迅速开展专项行动。

3. 新闻和出版管理部门

近年来，互联网新闻和出版管理部门积极配合公安机关、通信管理等部门，在打击网上淫秽色情、赌博等工作中，充分发挥职能作用，指导“互联网违法和不良信息举报中心”受理了大量群众举报，依法查处违法违规经营的互联网新闻信息服务单位，组织开展互联网上新闻宣传工作，在维护互联网秩序方面发挥了重要作用。

（1）国务院新闻办公室

国务院新闻办公室依照《互联网新闻信息服务管理办法》主管全国的互联网新闻服务监督管理工作。各省、市、自治区、直辖市人民政府新闻办公室负责本行政区域内的互联网新闻信息服务监督管理工作。对互联网新闻服务单位开办互联网信息服务进行审批，对其管理制度、人员资质和服务内容进行检查，对违规行为进行查处。

（2）新闻出版总署

我国新闻出版行业的主管机关，是国务院归口管理互联网出版的行政管理部门，对互联网相关领域的出版工作拥有监管职权。省、自治区、直辖市新闻出版行政部门负责本行政区域内互联网出版的日常管理工作，对本行政区域内申请从事互联网出版业务者进行审核，对本行政区域内违反国家出版法规的行为实施处罚。

4. 文化主管部门

负责对我国互联网文化领域进行监督和管理。省、自治区、直辖市人民政府文化行政部门主要负责本行政区内互联网文化活动的日常管理工作，对本行政区域内申请从事经营性互联网文化活动的单位进行初审，对本行政区域内申请从事非经营性互联网文化活动的单位进行审核，对本行政区域内互联网文化活动违反国家有关法规的行为实施处罚。

5. 广播电视行政部门

互联网视听节目服务的主管部门，负责对互联网视听节目服务实施监督管理，统筹互联网视听节目服务的产业发展、行业管理、内容建设和安全监管。

6. 药品信息和医疗卫生信息监管

对提供互联网药品信息服务活动的网站实施监督管理。

7. 国家互联网信息办公室

2011 年 5 月 4 日，国务院办公厅设立国家互联网信息办公室。其主要职责包括，落实

互联网信息传播方针政策和推动互联网信息传播法制建设，指导、协调、督促有关部门加强互联网信息内容管理，负责网络新闻业务及其他相关业务的审批和日常监管，指导有关部门做好网络游戏、网络视听、网络出版等网络文化领域业务布局规划，协调有关部门做好网络文化阵地建设的规划和实施工作，负责重点新闻网站的规划建设，组织、协调网上宣传工作，依法查处违法违规网站，指导有关部门督促电信运营企业、接入服务单位、域名注册管理和服务机构等做好域名注册、互联网地址（IP 地址）分配、网站登记备案、接入等互联网基础管理工作，在职责范围内指导各地互联网有关部门开展工作。

4.2.2 互联网信息内容安全管理法律框架

在法治社会中，法律法规作为规范一切社会关系的根本手段，同样也适用于网络社会。通过法律手段管理互联网具有稳定性和合法性，在法律意识浓厚的西方社会，自然成为互联网管理最根本性的、最为重要的手段，并且已成为世界各国的通行做法。“9·11”事件后，就网络信息安全领域加强立法成为各国的一个普遍趋势，在保障言论自由的基础上，都对互联网上出现的违法信息采取严密控制和严厉打击的措施，重点是对上网行为和网上内容进行监控和管理。

近年来，为进一步加大对互联网传播信息内容的安全管理，我国也注重大力推进互联网立法，并初步建立了互联网法律制度。目前，我国已经制定了《全国人大常委会关于维护互联网安全的决定》、《互联网新闻信息服务管理规定》等 30 多部针对互联网的法律、行政法规、司法解释和部门规章，基本形成了专门立法和其他立法相结合、涵盖不同法律层级、覆盖互联网管理主要领域和主要环节的互联网法律制度。

法律法规的制定为依法管理互联网提供了基本依据，为维护网络信息安全发挥了重要作用。目前，我国对互联网信息安全和信息内容安全的界定、管理手段、违法行为的处罚以及提供互联网服务、使用互联网的各种行为作出相应规定的法律法规主要包括：

(1) 1994 年 2 月 18 日，国务院第 147 号令发布了《中华人民共和国计算机信息系统安全保护条例》，这是我国第一部涉及计算机信息系统安全的行政法规。

(2) 1996 年 1 月 29 日，中华人民共和国公安部发布了《公安部关于对国际联网的计算机信息系统进行备案工作的通知》，进一步加强了对与国际联网的计算机信息系统的安全管理。

(3) 1996 年 2 月 1 日，国务院第 195 号令发布了《中华人民共和国计算机信息网络国际联网管理暂行规定》，加强对中华人民共和国境内的计算机信息网络国际联网安全保护的管理。

(4) 1997 年 5 月 20 日，国务院第 218 号令发布了《国务院关于修改〈中华人民共和国计算机信息网络国际联网管理暂行规定〉的决定》。对《中华人民共和国计算机信息网络国际联网管理暂行规定》进行了修正，其中加强了对于网络信息内容安全的管理和保护，并对使用网络传播非法不良信息的行为加重了处罚。

(5) 1997 年 12 月 8 日，国务院信息化工作领导小组审定了《中华人民共和国计算机信

息网络国际联网管理暂行规定实施办法》。该实施办法的主要内容是明确了国家发展互联网的战略规划和相应职能及管理权限的划分。

(6) 1997 年 12 月 16 日,公安部第 33 号令颁布了由国务院批准的《计算机信息网络国际联网安全保护管理办法》,这是我国第一部全面调整互联网络安全的行政法规,首次正式规定严格禁止利用国际联网危害国家安全、传播不良信息和进行计算机网络系统攻击等行为,并且对违反规定者明确了处罚措施。

(7) 2000 年 1 月 1 日,国家保密局发布了《计算机信息系统国际联网保密管理规定》,加强计算机信息系统国际联网的保密管理,确保国家秘密的安全。

(8) 2000 年 9 月 25 日,国务院第 292 号令公布了《互联网信息服务管理办法》,根据提供信息服务的性质(经营性或非经营性)以及所提供信息的类型,对开展业务所需符合的条件和履行的手续,以及传播内容等方面做了一些限制性规定。

(9) 2000 年 9 月 25 日,中华人民共和国国务院第 291 号令发布了《中华人民共和国电信条例》,规范了我国电信市场秩序,维护电信用户和电信业务经营者的合法权益,保障电信网络和信息的安全,促进电信业的健康发展。

(10) 2000 年 11 月 6 日信息产业部第 3 号令发布了《互联网电子公告服务管理规定》,规定开展电子公告服务业务必须经过专项备案或专项批准手续,并在电子公告发布的信息内容、上网用户个人资料保密等方面做出了规定。

(11) 2000 年 11 月 6 日,国务院新闻办、信息产业部发布了《互联网站从事登载新闻业务管理暂行规定》,促进了我国互联网新闻传播事业的发展,规范互联网站登载新闻的业务,维护互联网新闻的真实性、准确性、合法性。

(12) 2000 年 12 月 28 日,全国人大常委会发布了《全国人民代表大会常务委员会关于维护互联网安全的决定》,促进了我国互联网的健康发展,维护国家安全和社会公共利益,保护个人、法人和其他组织的合法权益。

(13) 2001 年 3 月 7 日,信息产业部发布了《关于进一步做好互联网信息服务电子公告服务审批管理工作的通知》。

(14) 2001 年 4 月 3 日,国务院办公厅发布了《国务院办公厅关于进一步加强互联网上网服务营业场所管理的通知》。

(15) 2002 年 11 月 15 日,中华人民共和国国务院第 363 号令发布了《互联网上网服务营业场所管理条例》,加强了对互联网上网服务营业场所的管理,规范经营者的经营行为,维护公众和经营者的合法权益,保障互联网上网服务经营活动健康发展,促进社会主义精神文明建设。

(16) 2003 年 12 月 8 日,中国互联网协会发布了《互联网新闻信息服务自律公约》,全国多家互联网新闻信息服务单位共同签署了该公约,承诺自觉接受政府管理和公众监督,坚决抵制淫秽、色情、迷信等有害信息的网上传播,抵制与中华民族优秀文化传统和道德规范相违背的信息内容。

(17) 2004 年 6 月 10 日,中国互联网协会发布了《互联网站禁止传播淫秽、色情等不良信息自律规范》。

(18) 2004 年 7 月 6 日,国家广播电影电视总局第 39 号令发布了《互联网等信息网络传播视听节目管理办法》,对通过信息网络传播视听节目的相关行为进行了规范。

(19) 2004 年 9 月 3 日,最高人民法院、最高人民检察院发布了《最高人民法院、最高人民检察院关于办理利用互联网、移动通信终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释》。

(20) 2004 年 12 月 22 日,中国互联网协会发布了《互联网搜索引擎服务商抵制淫秽、色情等违法和不良信息自律规范》。

(21) 2005 年 2 月 8 日,信息产业部发布了《非经营性互联网信息服务备案管理办法行政法规》,进一步促进了互联网信息服务业的健康发展。

(22) 2005 年 9 月 25 日,国务院新闻办公室、信息产业部联合发布了《互联网新闻信息服务管理规定》,对互联网新闻信息服务单位从事互联网新闻信息服务的相关行为进行了规范。

(23) 2005 年 12 月 13 日,公安部第 82 号令发布了《互联网安全保护技术措施规定》,对互联网服务提供单位、联网使用单位落实相应的安全保护技术措施作出了具体规定。

(24) 2006 年 2 月 28 日,信息产业部发布了《互联网电子邮件服务管理办法》,规范了互联网电子邮件服务,保障了互联网电子邮件服务使用者的合法权利。

(25) 2006 年 5 月 18 日,国务院第 468 号令公布了国务院法制办、国家版权局和信息产业部联合制定的《信息网络传播权保护条例》,该条例全面规范了信息网络引发的著作权法律问题,是我国信息化立法的又一里程碑。

(26) 2008 年,中国互联网协会发布了《中国互联网协会短信息服务规范》(试行),目的是为了规范短信息服务行业经营行为,维护用户的合法权益,促进短信息服务行业健康稳定发展。

4.2.3 互联网信息服务单位安全管理制度

对互联网信息服务单位提供的服务信息内容管理的范畴主要包括互联网站、互联网公共信息场所、互联网电子邮件服务、互联网娱乐平台服务、互联网点对点信息服务及互联网短信息服务等。

1. 互联网信息服务单位建立安全管理制度的法律依据

我国的互联网信息内容安全管理制度主要体现在《计算机信息网络国际联网安全保护管理办法》(公安部第 33 号令)的第四条、第五条、第六条、第七条、第十条、第十二条、第十四条、第十六条、第十七条、第二十一条和《互联网信息服务管理办法》(国务院第 292 号令)的第十四条、第十五条、第十六条的相关规定中。

2. 互联网信息发布单位信息发布、审核、登记制度

信息发布、审核，是指互联网信息发布单位在发布互联网信息时应进行审核，信息发布、审核的主体为信息发布单位，在我国通常包括网络接入单位，从事信息服务的联网单位，开办电子公告板、新闻组、提供广播式发送电子邮件功能的联网单位，使用公用账号的联网单位等。互联网信息发布单位所发布的信息不得含有色情信息及色情图片，不允许以散布暴力、凶杀或者教唆犯罪为目的，不能包含色情、反动、赌博、六合彩、影响民族关系、进行人身攻击或其他非法内容和令人反感的内容，且不能含有指向这些内容的链接。

首先，色情内容包括：任何面向 18 岁以上成年人的内容；成人色情内容；包含裸体或色情活动的图片、影像以及链接；粗俗或下流的语言。

其次，信息内容必须符合中国宪法的基本原则，杜绝出现损害国家荣誉、破坏社会安定的内容，如涉嫌分裂祖国、反党反政府的内容一律不予通过。

最后，含有法律、行政法规禁止的其他内容的，均不予审核通过。具体的审核工作由单位设立的信息审核员完成，信息内容的审核标准为《计算机信息网络国际联网安全保护管理办法》第 5 条的规定，信息发布单位必须根据该规定制定本单位的信息发布、审核、登记制度。

信息发布单位对本单位制作的信息或者委托其发布的信息要有审核手续。一般应由各权限部门、单位的负责人填写各单位《信息发布审核登记表》后，方可对外发布。制作和发布信息的单位和个人必须对其提供信息资料的合法性、真实性负责。信息发布单位对委托发布信息的单位和个人应进行登记，登记内容包括单位名称、委托人姓名、个人有效身份证号码、联系电话和委托发布信息类别及题目。

一般来说，信息的信源单位须凭单位介绍信，个人须凭有效身份证件办理委托发布信息的手续。信息的信源单位对提供的信息进行程序限定，限制带有某些不良词汇的信息发布。发现有害信息，信息发布单位应拒绝办理并及时报告当地公安机关。对以虚拟主机方式接入的单位，系统要做好用户权限设定工作，不能开放其信息目录以外的其他目录的操作权限。

我国现有法律、法规中，关于信息发布、审核、登记制度的规定一般相同，一些特殊信息服务的信息发布、审核、登记制度则有自己的特色，我国网络媒体信息内容的信息发布、审核、登记制度需按《互联网信息服务管理办法》第十四条的规定来进行。之所以要对信息内容及其相关资料、用户资料进行记录和备份的原因主要有两个，一是作为网络媒体服务商的正常安全措施，二是在发生安全事件时，作为响应和恢复的必要措施和证据。

此外，在互联网媒体内容涉及到国际联网时，应当遵循《计算机信息网络国际联网管理暂行规定》和《计算机信息网络国际联网安全保护管理办法》的规定，对委托发布信息的单位和个人进行登记，并对所提供的信息内容进行审核；建立计算机信息网络电子公告系统的用户登记和信息管理制度；在发布信息的相关单位和个人违反我国目前对于网络媒体信息内容的规定时，保留有关原始记录，并在 24 小时内向当地公安机关报告；按照国家有关规

定，删除本网络中含有违法内容的地址、目录或者关闭服务器；建立完备的接入单位和用户的备案制度。

3. 互联网站安全管理

1）互联网站安全保护管理制度

（1）建立用户、个人上网日志记录保存制度（交互式栏目记录：发帖用户 IP 地址、时间；主页修改访问记录：访问者的 IP 地址、起始时间和终止时间）。以上原始记录应至少保留 60 天，并在公安机关依法检查或查询时，予以提供。

（2）建立信息发布和链接网站审核、登记制度。网站对委托发布信息源的单位和个人进行登记，信息源单位需凭单位介绍信，个人需凭有效身份证件办理委托发布信息的手续；对信息源的单位提供的信息内容要依照《计算机信息网络国际联网安全保护管理办法》中第四条、第五条的规定进行审核；对本网站上的宣传主页及链接站点要经常进行检查，发现问题后应在 24 小时内报告当地公安机关网络安全保卫部门，备份后删除。

（3）建立聊天室、电子公告栏、留言板、个人主页上传服务等交式栏目的信息监视、保存、清除和备份制度。

（4）网站应建立由信息审核员（开办单位）、站长（ BBS 站）栏目主持人（各类栏目）组成的三级管理，分级负责制。开设 BBS 的网站应设专职的 BBS 站长，站长负责对栏目的设置、栏目主持人的资格进行严格考察，明确规定开办的栏目内容和范围；栏目主持人要加强对用户的正确引导和管理，对栏目信息要经常检查，发现重大事件及时报告。实行 7×24 小时监控制度，发现有害信息应做好备份并及时删除，同时报告公安机关。

① 栏目明确制度。网站应明确 BBS 开设的各具体栏目和类别，如时事论坛、网民聊天室、文化艺术类留言板、IT 行业布告栏、新闻跟帖等。

② 版主负责制度。网站开设 BBS 时应有专门人员对 BBS 实施有效管理。获准开展 BBS 的网站必须对获得批准的各个 BBS 栏目指定专职人员充当版主，每个栏目不得少于一个专职版主，并实行版主责任制。版主负责监管该栏目信息内容，除采取必要的技术手段外，应对登载的信息负有人工过滤、筛选和监控的责任。一旦发现 BBS 的栏目中有违法违规内容，将追究网站和该栏目版主的责任并予以处理。

③ 用户登记制度。提供 BBS 的网站应要求上网用户使用 BBS 前预先履行用户登记程序，填写网站提供的注册表格，提供真实、准确、最新的个人信息（包括姓名、电话、身份证号）。注册表格由网站妥善保存并不得随意泄露，用户注册后方可使用该网站提供的所有 BBS 栏目和相关服务。一旦发现用户违反规定或提供虚假信息，网站有权暂停或中止该用户使用本网站包括 BBS 在内的所有或部分服务。

④ 规定张贴制度。开办 BBS 的网站在留言板、论坛、聊天室、跟帖等 BBS 网页的显著位置张贴 ICP 经营许可证号或备案号。点击经营许可证号或备案号，应弹出该经营许可证或备案表的清晰可认的扫描图片。上网使用者点击 BBS 某一栏目时，应首先弹出载有电子公告服务规则的页面，该页面内容旨在对使用者的行为作出符合法律规范和政府要求的警

示和限定，其中包括 2000 年 12 月 28 日第九届全国人大常委会第十九次会议通过的《全国人民代表大会常务委员会关于维护互联网安全的决定》有关条款。对 BBS 用户发出的信息应预先进行软件自动过滤和人工过滤。

(5) 建立搜索引擎安全保护管理制度。规范搜索引擎搜索网站的行为，对每一个上挂网站均要进行登记并报网站安全组织相关负责人审批。

(6) 建立异常情况及违法犯罪案件报告和协查制度。落实案件、事故报告和调查协助工作机制，凡发现有违反国家法律法规的行为，应保留有关原始记录，做好数据备份，并于 24 小时之内向当地公安机关报告。重大案件和事故应立即报告，并配合公安机关做好调查处置工作。

(7) 建立安全教育和培训制度。对网站相关部门的安全专管员、技术员等进行定期或不定期的安全教育和培训，积极参加公安机关开展的专题安全培训工作，并建立培训台账。

(8) 建立重要网络系统的系统备份及应急预案制定。针对网站实际建立信息网络重大事故案件应急预案工作机制，定期或不定期进行演习，并建立工作台账。

2) 互联网站安全保护技术措施

(1) 保存 BBS、论坛、留言板、聊天室等交互式栏目日志记录。

(2) 保留用户登录、退出、文件传输等日志记录 60 日以上。

(3) 能够对特定 IP 地址进行阻断。

(4) 能够限制来自相同客户端 IP 的最大同时连接数量和最大连接频率。

(5) 能够对标题、内容等进行基于特征字符串的过滤。

(6) 支持过滤规则动态导入和维护，并立即生效。

(7) 对过滤和阻断的信息数量可以进行统计，对公安机关所要求的过滤信息可以向公安机关传送。

(8) 保存网站维护及 FTP 日志记录。

4. 互联网公共信息场所安全管理

互联网公共信息场所是指通过电子公告、BBS、论坛、网络聊天室、网页制作、即时通信等交互形式，为上网用户提供信息发布条件，为上网用户提供信息的公共场所。

1) 网上公共信息场所运营单位安全保护管理制度

(1) 信息先审后发制度。要求运营单位通过人工或者技术的方式对用户发布在网上公共信息场所的信息实行先审后发。

(2) 信息巡查报告制度。要求运营单位实行 7×24 小时信息巡查制度，发现有害信息做好备份并及时删除，同时报告公安机关。

(3) 用户身份登记制度。要求运营单位对上网用户使用 BBS、聊天室、即时通信等服务的履行用户登记义务，填写注册表格，提供真实、准确、最新的个人信息(包括姓名、电话、身份证号)。注册信息由运营单位妥善保存并不得随意泄露，用户注册后方可使用 BBS 栏目和相关服务。一旦发现用户违反规定或发布有害信息，有权暂停或中止该用户的全部或者

部分使用服务的权限。

（4）异常情况及违法犯罪案件报告和协查制度。落实案件、事故报告和调查协助工作机制，凡发现有违反国家法律法规的行为，应保留有关原始记录，做好数据备份，并于24小时之内向当地公安机关报告，重大案件和事故应立即报告，并配合公安机关做好调查处置工作。

（5）安全教育和培训制度。对公共信息场所相关部门的安全专管员、技术员等进行定期或不定期的安全教育和培训，积极参加公安机关开展的专题安全培训工作，并建立培训台账。

（6）重要网络系统的系统备份及应急预案制度。针对网上公共信息场所实际建立信息网络重大事故案件应急预案工作机制，定期或不定期进行演练，并建立工作台账。

2）网上公共信息场所运营单位安全保护技术措施

（1）保存BBS、论坛、留言板、聊天室等交互式栏目日志记录。

（2）保留用户登录、退出、文件传输等日志记录60日以上。

（3）能够对特定IP地址进行阻断通信。

（4）能够限制来自相同客户端IP的最大同时连接数量和最大连接频率。

（5）能够通过标题、内容等进行基于特征字符串的过滤。

（6）支持过滤规则动态导入和维护，并立即生效。

（7）对过滤和阻断的信息数量可以进行统计，对公安机关所要求的过滤信息可以向公安机关传送。

5. 几类特定互联网信息服务单位安全保护管理制度及技术要求

1）互联网电子邮件服务单位

互联网电子邮件服务单位安全管理应落实下列安全保护管理制度及技术措施：

（1）网络安全漏洞检测和系统升级管理制度。必须定期对电子邮件服务器进行安全漏洞检测，同时对系统进行升级。

（2）操作权限管理制度。规范管理电子邮件服务器管理员的管理权限，确保责任落实到人。

（3）用户登记、验证制度。用户必须注册后才可使用电子邮箱。对外提供电子邮件服务的，用户的注册资料必须包括用户的手机或常用的电子邮箱，网站必须对用户注册的手机或电子邮箱进行验证；对单位内部提供电子邮件服务的，负责电子邮件服务开设的管理员必须妥善保管用户递交的电子邮件开通申请或开通登记表中用户的姓名及联系方式等信息。

（4）建立应急处置预案。有关单位应当建立对网络突发事件的应急处置预案。

（5）报警制度。对电子邮件服务器中发生的安全事故及各种违法事件，维护单位应当采取应急处置预案，保留有关原始记录，在24小时内向所在地公安机关网络安全保卫部分报告。

（6）协查制度。公安机关行政执法过程中，有关单位应当如实提供有关资料，并提供相关技术支持和必要协助。

(7) 联络制度。设定专人 24 小时与公安机关保持畅通的联系渠道，联系方式必须包括：手机、值班电话、电子邮箱，如有变更，应及时与公安机关联系。

(8) 告知制度。应当将电子邮件服务和使用规则告知用户，服务商应向用户公示举报和投诉有害垃圾电子邮件的方式，建立反有害垃圾电子邮件工作制度；同时还应公布公安机关的举报电话和举报电子邮箱。

(9) 具备垃圾电子邮件清理功能。

(10) 能够通过在线或者离线两种方式向公安机关提供有害垃圾电子邮件。其中在线传送方式由公安机关提供垃圾电子邮件数据通信软件。

2) 互联网娱乐平台服务单位

互联网娱乐平台是指以公共信息网络为平台，发行、运营互联网网络游戏和互联网网络游戏开发、代理、运营的服务平台。互联网娱乐平台服务单位安全管理应落实下列安全保护管理制度及技术措施：

(1) 建立用户发布信息责任公告制度和有害信息用户举报渠道。

(2) 发生网络安全事故、事件的报告制度。

(3) 发现含有有害信息的地址、目录或者服务器时，应当通知有关单位关闭或删除。

(4) 建立健全网上违法犯罪案件协查工作制度。

(5) 留存用户注册信息，记录用户登录和退出的网络地址、时间并留存 60 日。用户自己注销账户后，该账户信息及其之前上网记录应保留 60 日后再删除。

(6) 基于关键词的有害信息过滤、删除、留存措施。

(7) 基于特定用户账号的登录报警措施。

(8) 落实重点网络游戏用户实名制和网络游戏用户虚拟财产保护措施。

3) 互联网点对点信息服务单位

互联网点对点信息服务是指中华人民共和国境内以点对点共享网络为平台，进行点对点文件共享和数据交互以及其他点对点的信息应用。互联网点对点信息服务单位安全管理应落实下列安全保护管理制度及技术措施：

(1) 建立用户发布信息责任公告制度和有害信息用户举报渠道。

(2) 建立信息安全管理人员教育和培训制度。

(3) 建立信息员，构建工作关系、朋友关系。

(4) 留存用户注册信息，记录用户登录和退出的网络地址、时间并留存 60 日。

(5) 信息发布、信息搜索、消息广播和文件共享服务中对有害信息基于关键词和文件哈希值的过滤。

(6) 客户端软件记录用户共享文件信息被其他用户(包括 IP 地址、账号等)下载的时间和次数；服务器端具有远程调取客户端记录，并记录文件或信息最初发布者网络地址、用户账号和发布时间的功能。

(7) 基于特定用户账号的登录报警。

4）互联网短信息服务单位

互联网短信息服务是指中华人民共和国境内通过移动通信运营商和互联网信息服务单位提供的信息交换平台进行文字、图片等短信息交流的服务。互联网短信息服务单位安全管理应落实下列安全保护管理制度及技术措施：

（1）应依法履行备案手续，定期报送备案存档资料。移动、联通等基础电信业务经营商应当在规定日期内将互联网短信息服务单位的有关资料按照固定的格式报送公安机关网络安全保卫部门存档；互联网短信息服务单位在开通服务的同时准备好相关备案材料，并报送公安机关网络安全保卫部门备案。

（2）逐步落实互联网短信息实名制，督促、指导移动、联通等基础电信业务经营单位和互联网短信息服务单位落实用户实名登记制度，完善个人身份信息登记款项。

（3）建立有害互联网短信息的防控长效机制。督促各互联网短信息服务单位积极配合公安机关打击互联网短信息违法犯罪，通过互联网短信息和本单位网站开辟报警服务栏目的方式，公布有害互联网短信息举报受理的范围和方式。

（4）建立信息巡查制度。督促、指导互联网短信息服务单位建立信息巡查制度，对提供下载的公共互联网短信息进行巡查，发现敏感短信息及时取证、删除。

（5）记录用户发送的短信内容、时间、源地址和目标地址并保存信息60日以上。

（6）对具有以下特征的互联网短信息的监测报警和封堵过滤功能：同一用户名超过最大发送数量的短信息；同一用户名超过最大发送频率的短信息；短信息发送/接收的用户名、手机号码包含设定的过滤内容；短信息内容包含设定的过滤关键词。

（7）对短信息发送/接收的用户名、手机号码及短信息内容等信息60日日志留存；对被封堵、过滤的短信息发送/接收的用户名、手机号码和短信息内容等信息60日日志留存（同一特征抽取一条）；公安机关对留存数据库能够远程查询访问。

4.3 互联网有害信息查处

互联网的快速发展使得人们更加便捷地获取信息，然而大量的色情、暴力以及恐怖主义等有害内容也在网络上泛滥肆虐，这些有害信息的泛滥使得互联网信息内容安全得到了广泛的关注。

4.3.1 互联网有害信息的概念和特征

1. 互联网有害信息的概念

互联网上的有害信息，是指互联网上一切可能对现存法律秩序和其他公序良俗造成破坏或者威胁的数据、新闻和知识等信息。

2. 互联网有害信息的特征

互联网有害信息具有以下特征：

（1）互联网有害信息包括破坏或威胁现存法律秩序的信息和违背其他公德良俗的信息两大类。

（2）互联网有害信息包含着对客观事实的主观价值判断的成分。有害信息首先是对网络上客观存在的数据、新闻、知识等事实的描述，因而其包含客观内容。某一事物有害还是无害，又包含着主体对认识对象的主观价值判断成分。现代社会价值判断标准日趋多元化，不同的人从不同的角度，站在不同的立场上，对同一客观事物的善恶褒贬的看法很可能不同。因此，有害还是无害是相对的，会因人而异。所谓的有害信息，是以现存法律秩序和社会公共道德为标准而得出的结论。

（3）互联网有害信息的范围具有可变性。由于有害信息包含价值判断的成分，而价值判断标准是多元的，因此，有害信息的具体内容会随着社会主流意识的变迁而更迭。当立法者的观念发生变化，或者社会道德标准、风俗出现转折的时候，价值判断标准也随之改变，有害信息的具体内容也会随之改变。因此，对互联网上有害信息的界定应当注意与时俱进，不可因循守旧。

4.3.2　互联网有害信息的界定

1. 国外有关互联网有害信息的规定

世界各国对互联网有害信息的提及由来已久，欧盟委员会于 1996 年 10 月和 1996 年 11 月发表的《在视听和信息服务中保护未成年人和人类尊严绿皮书》和《关于因特网非法和有害内容的通讯》两个重要文件，是欧盟及其成员国为反对利用因特网向未成年人传播暴力和色情等内容而采取的行动。其实每个国家对有害信息都有自己的定义：

（1）英国的比较有代表性，它把有害信息分为三类：一类是非法信息，指危害国家安全等国家法律明令禁止的信息；一类是有害信息，比如说鼓励或教唆自杀的信息，虽然没有纳入到非法的信息里面，但是它已经是有害信息；还有一类就是令人厌恶的信息，例如色情信息。

（2）新加坡政府规定，危害公共安全、破坏民族和宗教和睦关系、违背公共道德的信息为有害信息。

（3）美国、法国、加拿大、澳大利亚等国家都通过立法等形式，将色情、暴力、危害国家安全、煽动种族和宗教仇恨歧视等信息明确定义为有害不良信息。

欧盟委员会还于 1997 年制定了《关于促进因特网安全使用的多年度统一行动计划》，进一步提出打击非法和有害信息的计划，并确认八类信息内容为非法或有害信息。

2. 我国现行法律法规中对互联网有害信息的界定

1）《计算机信息网络国际联网安全保护管理办法》规定

第五条　任何单位和个人不得利用国际联网制作、复制、查阅和传播下列信息：

① 煽动抗拒、破坏宪法和法律、行政法规实施的；

② 煽动颠覆国家政权，推翻社会主义制度的；

③ 煽动分裂国家、破坏国家统一的；
④ 煽动民族仇恨、民族歧视，破坏民族团结的；
⑤ 捏造或者歪曲事实，散布谣言，扰乱社会秩序的；
⑥ 宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的；
⑦ 公然侮辱他人或者捏造事实诽谤他人的；
⑧ 损害国家机关信誉的；
⑨ 其他违反宪法和法律、行政法规的。

2)《互联网信息服务管理办法》规定

第十五条　互联网信息服务提供者不得制作、复制、发布、传播含有下列内容的信息：
① 反对宪法所确定的基本原则的；
② 危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；
③ 损害国家荣誉和利益的；
④ 煽动民族仇恨、民族歧视，破坏民族团结的；
⑤ 破坏国家宗教政策，宣扬邪教和封建迷信的；
⑥ 散布谣言，扰乱社会秩序，破坏社会稳定的；
⑦ 散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；
⑧ 侮辱或者诽谤他人，侵害他人合法权益的；
⑨ 含有法律、行政法规禁止的其他内容的。

3)《中华人民共和国计算机信息网络国际联网管理暂行规定》规定

第十三条　从事国际联网业务的单位和个人，应当遵守国家有关法律、行政法规，严格执行安全保密制度，不得利用国际联网从事危害国家安全、泄露国家秘密等违法犯罪活动，不得制作、查阅、复制和传播妨碍社会治安的信息和淫秽色情等信息。

4)《互联网新闻信息服务管理规定》规定

第十九条　互联网新闻信息服务单位登载、发送的新闻信息或者提供的时政类电子公共服务，不得含有下列内容：
① 违反宪法确定的基本原则的；
② 危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；
③ 损害国家荣誉和利益的；
④ 煽动民族仇恨、民族歧视，破坏民族团结的；
⑤ 破坏国家宗教政策，宣扬邪教和封建迷信的；
⑥ 散布谣言，扰乱社会秩序，破坏社会稳定的；
⑦ 散布淫秽、色情、赌博、暴力、恐怖或者教唆犯罪的；
⑧ 侮辱或者诽谤他人，侵害他人合法权益的；
⑨ 煽动非法集会、结社、游行、示威、聚众扰乱社会秩序的；
⑩ 以非法民间组织名义活动的；

⑪ 含有法律、行政法规禁止的其他内容的。

4.3.3 互联网有害信息处置

对互联网有害信息的处置是公安机关维护健康有序网络环境的重要手段。

1. 互联网有害信息处置工作内容

互联网有害信息的处置工作包括有害信息的证据固定和信息处理。

发现网上有害信息和有害网站，应立即进行证据固定，保留原始资料。证据固定的具体要求和方法如下：

1）证据固定要求

（1）遵循依法收集、客观全面、迅速及时、细致入微、掌握重点的原则进行。

（2）必须由两名以上执法人员共同进行。

2）证据固定的具体方法

（1）对有害信息进行屏拷。

屏拷是对互联网有害信息进行证据固定最常用的方法，屏拷时要符合以下要求：对所需要的信息进行屏拷时，如因信息页面太大而进行分屏屏拷时，要保证信息的连贯性；屏拷时，要对证据固定时所用的互联网终端的任务栏进行隐藏，屏拷后的页面上不能出现任务栏信息；屏拷后的图片大小以能看清信息内容为准（通常将打印纸的左右页边距分别设为2cm，上下页边距分别设为3cm，同时在一页纸上放置两幅屏拷图，且两图之间要留有一行空行）；屏拷后形成的证据文件打印页上要留有一定的空白位置，以供有关人员确认；屏拷时，要对每一次操作进行相关动作的文字说明。

（2）互联网信息场所上的信息经屏拷后必须打印，并由与该网上行为有关的责任人签字、盖章确认，同时在必要的时候，要将有关打印件送相关鉴定部门进行鉴定才能成为有效证据。

（3）互联网信息场所信息取证结合其他证据必须能证明以下事项：行为人的身份，行为是否存在，行为是否为行为人所实施，实施行为的时间、载体、手段、后果及其他有关情节，行为人的责任及共同行为人的责任，行为人实施行为情节的轻重，其他与行为有关的事实。

（4）对互联网信息场所信息的证据固定要采取备份措施。

对有害信息的处理方法，总体上分为行政方法、技术方法、谋略方法三种，互联网信息内容安全管理工作中发现有害信息后，应视不同情况采取这三种方法中的一项或者多项处置措施。

2. 互联网有害信息处置工作要求

1）把握尺度，内紧外松

有害信息的处置要把握政策尺度，做到“内紧外松”，即根据有关政策对有害信息研判定性准确，不致使打击面过大，对出现的有害信息要认真对待、严肃处置，对外要不事张扬防止炒作。

2）及时防御，快速处置

互联网信息的特点是传播速度快、传播范围广，在有害信息处置工作中要做到及时防

御、快速处置，避免有害信息扩散，造成不良的社会影响。

3）措施得当，方法到位

在有害信息处置工作中，要分析有害信息的性质，根据有害信息的传播情况、社会危害性等，作出合理到位的处置。在处置中要注意工作方法，防止因处置不当造成负面影响。

4.3.4 互联网有害信息举报投诉及案件报告与协助查处制度

1. 有害信息举报投诉制度

有害信息举报投诉制度设立的目的是为了鼓励公众举报互联网违法和不良信息，这是公众参与管理互联网原则的体现，属于公众监督的范畴，其最终的目的是维护社会公共利益。有害信息举报投诉制度对推动行业自律、加强互联网依法管理有重要意义。

我国已建立有害信息举报投诉制度。公安部专门设立了“网络违法犯罪举报网站(http://www.cyberpolice.cn)”，其举报受理范围包括：

（1）进行邪教组织活动、煽动危害国家安全的；

（2）散播谣言，侮辱、捏造事实，扰乱社会秩序的；

（3）传播淫秽色情信息，组织淫秽色情表演，赌博、诈骗、敲诈勒索的；

（4）侵犯他人通信自由、通信秘密的；

（5）网络入侵、攻击等破坏活动的；

（6）擅自删除、修改、增加他人数据的；

（7）其他网络违法犯罪活动。

2. 案件报告与协助查处制度

（1）案件报告制度

互联单位、接入单位及使用计算机信息网络国际联网的法人和其他组织，若有发现《计算机信息网络国际联网安全保护管理办法》第五条中规定之有害信息时，应当在保留有关原始记录后及时予以删除，并在 24 小时内向当地公安机关报告；发现计算机犯罪案件，立即向公安机关网络安全保卫部门报案，并保护好现场。

（2）协助查处制度

协助查处制度，是指互联单位、接入单位及使用计算机信息网络国际联网的法人和其他组织应协助公安机关做好计算机违法案件调查取证工作和对网络用户处罚的执行工作，在接到公安机关对某网络用户进行停止联网或禁止入网的通知时，立即予以执行。

4.4 互联网热点信息管理

4.4.1 互联网热点信息的概念和特征

1. 互联网热点信息的概念

随着信息传播手段的进步，尤其是互联网的出现，人们已经由信息贫乏进入到一个信息

极度丰富的时代。面对不断涌现的新信息，人们迫切需要从中得到自己想要的信息。热点信息是指某段时间内各个领域发生的引起人们较大关注的话题信息。

互联网热点信息则是网民思想情绪和群众利益诉求在互联网上的集中反映，是网民热切关注的聚焦点，是民众议论的集中点，反映出一个时期网民的所思所想。

互联网热点信息紧扣社会舆情，往往是社会重大事件，或是与群众切身利益密切相关的问题，很容易在短时间内引起网民广泛关注，对现实社会产生深刻影响。所以，发现并监控热点信息有助于让大众知晓某段时间内的社会焦点，及时地发现社会舆情，为监管部门制定相关政策提供理论依据，对于构建社会主义和谐社会具有重要意义。

2. 互联网热点信息的特征

在当前的社会舆论中，热点问题最引人注目，它矛盾复杂、是非莫辨，往往成为公众情绪的“催化剂”，社会舆论的“牛鼻子”，涉及整个舆论的走向。热点问题具有以下特征：

(1) 普遍性。社会热点是社会经济生活中普遍存在的现象，有的还涉及群众的切身利益，因而引起了社会各方面的广泛关注。

(2) 时代性。社会热点是改革开放的伴生物，它迅速反映客观世界的最新动向与最新趋势，在诸多的社会矛盾中，热点问题比较突出，使人无法回避。

(3) 挑战性。热点、难点问题，是改革开放过程中一些深层次矛盾的显露，解决这些问题有相当难度，对领导者与实际工作部门极富挑战性。

(4) 敏感性。由于是深层次矛盾的爆发，因此，多数热点问题相当敏感，是社会上一根“紧绷的弦”。

(5) 突发性。热点事件在某个时间段内能引起人们极大的关注，事件传播迅速，盛行一时。

(6) 流变性。随着情况的发展与公众关注点的变化，热点问题也会转化，其自身有发生、发展、消退的过程，今天是热点，明天就可能不是，又有新的热点问题取而代之。

4.4.2 互联网热点信息的搜集与编报

1. 信息搜集的主要方法

1) 巡查

(1) 通过 IE 等网络浏览器，在地址栏中直接输入网站的 IP 地址或域名，可直接查看网站的内容。对新闻类网站、门户网站、校园网站、综合网站、社区论坛、校园论坛、专业论坛等各类网站的网页等网上信息场所进行巡查，对其发布的信息进行甄别、筛选、归类和统计。

(2) 使用互联网上通用的搜索引擎，如 Google、Baidu、Yahoo、中搜、一搜等，针对相关信息内容的关键字在搜索数据库进行关联查询，在数据库内查找到相关联的信息后，再链接到所对应的网络地址，从而获取所需要的信息。

(3) 通过公安机关网络安全保卫部门专门配备的搜索引擎工具，使用一定的关键词关联，在一定网段内、事先设定的网站上自动巡查、下载含有关键词的网上信息或网页。

2）技术手段监控

通过报警处置分布式监控系统、网吧监控软件以及其他特定网络技术手段对特定网站、境外已封堵网站、重点单位的后台数据、互联网信息服务场所等信息情报进行搜集。

3）保留原始网页

将其网页上有关敌情、政情及社情等类别的信息进行提取，并保留原始网页。对论坛中出现的情报信息，存留时必须保留其题目在论坛中出现位置和具体内容的原始网页。

4）其他方法

（1）主动发帖与网络用户进行交流搜集获取。

（2）刺激特定对象反应搜集获取。

（3）对特定对象的网络 ID 进行控制监视获取。

（4）通过加入网络组织、注册成为网站会员等主动获取。

（5）通过订阅网络杂志、网络期刊、网络短信等被动获取。

（6）通过网络信息的结果推断、判定网络活动的因果关系获取。

（7）通过秘密力量搜集获取。

2. 信息搜集的要素

（1）对论坛、BBS 上的信息，搜集的基本要素包括：

① 发现时间，信息所在论坛的频道、栏目，信息所在网站的 IP 地址和服务器所在地，信息所在网页的 URL，对新出现的网站或第一次发现的网站，要查明网站基本情况或背景情况。

② 发帖人名称（网名或真实姓名）、发帖时间（煽动性信息具体到秒）、信息标题，简述帖子主要内容和主要观点。

③ 帖子浏览量（点击率）；是否引起网民讨论或跟帖，跟帖量，主要讨论情况（主要观点及其信息比例）；是否被转贴到其他网站、论坛上，其他网站传播、转贴、张贴情况及其讨论情况，讨论中是否出现煽动性信息，具体列举煽动性信息。

④ 是否采取处置措施或通报有关部门采取处置措施，处置情况（删除的具体时间、初步调查情况等）。

⑤ 原始网页的内容以单一网页或 Word 文档作为附件。

（2）对新闻网站、门户网站上的信息，搜集的基本要素包括：

① 发现时间、新闻网站、栏目报道、刊登时间、信息标题、信息所在页面的 URL、信息主要内容（评论性信息要注明相关人员姓名和身份；事件性信息要具备时间发生时间、地点，涉及主要人物，事件起因、经过和结果），只有转载新闻权的网站上的新闻报道，要注明信息来源。

② 在新闻跟帖中是否引起网民评论、议论，有关评论、议论信息数量，主要观点及其比例。如果引起网民持续关注，每日（时）评论、议论增加数量和趋势。

③ 引起网民关注的信息在其他网站上的情况。

④ 信息原文以单一网页或 Word 文档作为附件。

(3) 对其他网站上的信息,参照上述类似网站上信息的基本要素进行搜集。

3. 信息编报

互联网信息编报是根据不同的需求和方法,在互联网信息搜集、分析研判的基础上,将互联网信息编写成文,向有关领导和情报信息使用单位上报、送达、下发的过程。编写质量的高低好坏,直接影响到互联网信息的使用。

编报社会热点信息动态时,应注意以下几个方面:

1) 热点问题冷静思考

冷与热是相对的,辩证的。在改革开放时期,各种新现象、新矛盾、新动向的出现并不奇怪,要从大局出发,对热点进行理性思考,切不可草率编报。热点问题往往因触及各种利益关系而变得十分敏感,人们议论纷纷、莫衷一是,它是社会心态与公众情绪的“晴雨表”。因此,信息编报工作人员首先要提高政治敏锐性与观察力,以政治眼光对热点问题进行估量,尤其是对某一个时期的热点问题,要了解网上舆论,各种议论、意见、建议及锋芒所向,作出正确的判断;要正确把握热点问题的本质所在;要对产生热点问题的诸多因素的来龙去脉、发展趋势作深入了解;对热点问题与其他事物间的互相联系、互相依存、互相转化的方面也要有全面的了解。编报社会热点信息动态还涉及对象的美丑、真假、善恶、好坏、利弊,涉及伦理道德、价值取向、人文精神等内涵。

2) 透过现象抓住本质

在热点报道中,不能满足于抓现象,而是要从现象入手,层层剥笋,牢牢抓住事物的本质。许多成功的热点问题报道,都是透过纷繁复杂的社会现象,从局部到整体,从事物的外部联系深入到事物的内核,通过事实的交融升华,揭示事物本质,从而帮助使用者获得对热点问题的规律性认识。

3) 共性着眼,个性着手

在热点编报中,要处理好矛盾的普遍性就是共性与矛盾特殊性即个性的辩证关系。热点问题,一定要从个性着手,从共性着眼,把宏观与微观巧妙地结合起来。如果热点编报选择的是个别的、孤立的、偶然的事实,割裂了事物间的内在联系,就事论事地去报道,只能使使用者“一叶障目,不见泰山”。

人们认识事物的时候,首先是从个性开始。社会热点问题,由于吸引了千百万人的视线,因此具有鲜明的个性特征。抓热点,首先要抓矛盾的特殊性,这是认识规律,事物的个性是离不开共性的。在进行热点编报时,一定要高屋建瓴,善于从全局上衡量被编报的问题是否具有普遍意义、指导意义。

对热点问题的报道,还要抓准“点”,这个“点”如果没有时代意义,没有代表性,没有体现共性,那就失去了价值。大千世界充满着各种矛盾与冲突,大至局部战争,小至邻里纷争,都可形成热点问题。因此,在众多的热点问题中,要认真鉴别与分析,哪些问题具有矛盾的普遍性,既是领导关注的,又是实际工作部门瞩目的,更是群众议论纷纷的,其显露的倾向具有

普遍性,其蕴涵的实质具有指导性。

4）善于分析解剖矛盾

在抓住事物的本质后,要下工夫把“质”分析好。要善于应用辩证唯物主义和历史唯物主义的世界观与方法论,对社会热点的来龙去脉、前因后果作深刻的分析。分析的过程,就是解剖矛盾的过程,就是摆事实、讲道理的过程,要摒弃线性单一因果律的思维方式。构成社会热点的因果关系是比较复杂的,不能用“非此即彼”、“一因一果”的编报方式来反映。

5）切忌片面,把握好“度”

热点问题的编报,要讲究科学性,忌片面性,关键的问题是把握好“度”。要坚持唯物辩证法,用全面、发展的眼光来观察事物、分析问题。既要看到事物的正面,又要看到其反面;既要看到事物的主流,又要看到其支流;既要看到主要矛盾,又要看到次要矛盾;既要看到事物的现状,又要预测其发展前景。要辨究分寸、角度、时机,把握火候,既避免“不及”,又力戒“过头”。任何事物都有极限,突破了上限或下限,就要导致谬误。

习　　题

1. 简要说明我国互联网信息内容安全管理的机构及职责。
2. 简要说明互联网有害信息是如何界定的。
3. 简要说明互联网有害信息固定证据的方法是什么。
4. 简要说明互联网热点信息的特征有哪些。
5. 简要说明信息搜集的主要方法。

第 5 章

互联网上网服务营业场所安全管理

【内容提要】

本章主要介绍互联网上网服务营业场所安全管理的相关内容，通过分析互联网上网服务营业场所存在的安全问题，以《互联网上网服务营业场所管理条例》为执法依据，从互联网上网服务营业场所信息网络安全管理、治安安全管理和消防安全管理等方面阐述安全管理制度和技术措施。通过学习，掌握互联网上网服务营业场所的安全监管工作及行政处罚等方面的规定。

5.1 概　　述

互联网上网服务营业场所作为最便捷的触网终端场所进入网民视野，并一度成为仅次于家庭、办公场所之外的网民第三大上网场所。在为人们提供高效、快捷、便利的服务和体验的同时，也必然引发诸多的社会问题，互联网上网服务营业场所能否持续、健康、稳定的发展，与政府的管理、经营单位的经营行为有着直接的关系。

5.1.1 互联网上网服务营业场所及发展概况

1. 定义

互联网上网服务营业场所是指通过计算机等装置向公众提供互联网上网服务的网吧、计算机休闲室等营业性场所。

2. 主要特征

（1）向公众提供上网服务

服务的对象是否为公众，是认定其是否为互联网上网服务营业场所的重要依据。也就是说，互联网上网服务营业场所的服务对象是不特定的人群，而且其服务范围也是不特定的和开放式的。一般社区、学校、图书馆、宾馆、咖啡屋、娱乐休闲中心等向特定对象提供上网服务的场所不纳入互联网上网服务营业场所的管理范围。

有些互联网上网服务营业场所由于自身经营需求而采取“会员制”等形式以确保拥有相对固定的消费群体，并不改变其为公众提供上网服务的性质。

2）以赢利为目的

这是互联网上网服务营业场所的经济特征。互联网上网服务营业场所自诞生之日起就是以赢利为目的，有些经营者甚至为了赢利而采取各种刺激消费的手段。

这里面包含两方面的含义：一是指投资人建立互联网上网服务营业场所的目的是为了获得利润，即使经营亏损甚至倒闭也并不影响其赢利性的特征；二是指应当在一定时期内连续从事互联网上网服务活动，即经营内容相对固定化。

3. 发展概况

互联网上网服务营业场所目前工作的管理对象主要是面向公众的网吧。网吧的发展主要经历了以下几个阶段。

1）1995 年之前——兴起阶段

国内的网吧刚刚兴起，主要代表为上海的国内首家网吧 3C＋T，此时的经营形式主要模仿台湾的网吧，走的是网络咖啡屋模式，功能上大多只有上网终端服务和有限的游戏娱乐服务，部分网吧也提供饮料、食品等额外服务项目。网吧用户对象大多为高校师生、企业职员以及外籍人士。由于个人上网不便和所需的费用以及设备价格过高，网吧成为人们获取网络资源的最好场所。当时的网吧规模非常有限，消费价格相对较高，一般为每小时 20 元左右。

2）1995—1998 年——高峰阶段

这一阶段网吧不再是单一的上网场所，开始向游戏类娱乐场所发展。用户群体开始增加，不少时尚青年开始以网吧提供的游戏服务作为重要的娱乐手段，使网吧行业获得了巨大的客源与需求。由于网吧数量的发展和相互竞争的需要，网吧消费水平开始降低，一般为 10 到 15 元，服务内容也开始以单机游戏为主，上网服务由于并没有更大的用户群体扩充而成为网吧的次要服务项目。此时的网吧规模一般都维持在 10 至 20 台计算机之间，鲜有 40 台计算机以上的网吧出现，网吧的形式也趋于本地化和简陋化。

3）1998—2000 年——膨胀阶段

国内网吧的数量开始迅速增加，从而引起了大规模的行业内竞争。而此时的网吧间竞争已不再是单一的价格战，网吧业主开始在上网速度、硬件设备、上机价格上进行大规模的宣传与竞争。最终导致网吧消费水平直线下降。在这种情况下，网吧又纷纷推出通宵上机优惠、包时限优惠等措施，而在管理上大大放手，使网吧成为一系列社会问题滋生的温床，同时在此期间网吧行业发展开始变缓，开始淘汰大批竞争中的失败者。

4）2000—2002 年——第二次高峰阶段

2000 年，一种新型的娱乐形式——网络游戏在国内开始流行，网吧开始接纳既需要游戏，又需要上网的玩家群体，使网吧行业的用户进一步扩展。经过了 2000 年前的网吧大战后，2001 年上海东方网点连锁管理有限公司成立，各地也开始了连锁网吧的建设，不少地区网吧也自发地结合成网吧联盟体系，开始了在网吧连锁化经营上的尝试。网吧行业开始有所复苏，并开始接纳大量的网络游戏玩家。

5）2002 年以后——正规化发展阶段

由于上网用户的增加，使网吧放松管理所带来的弊病开始显现。2002 年 6 月，北京“蓝极速”事件爆发后，国家有关部门开始加大对网吧行业的监管力度。同年国务院颁布了《互联网上网服务营业场所管理条例》，使网吧行业开始了重新洗牌阶段。网吧发展数量开始受到严格管理，缺乏管理的非正规中小型网吧关、停、并、转，网吧行业进入正规化发展前的阵痛阶段。网吧价格开始回涨，并达到了一个相对稳定的平民价格。

2003 年，文化部发布了《文化部关于加强互联网上网服务经营场所连锁经营管理的通知》，为网吧行业的发展指明了道路，国内网吧行业正式开始了连锁化的发展道路。虽然此前在全国各地都出现过网吧连锁店的形式，但大多没有正规的连锁化实质内容。而国内网络游戏在 2002 年后也开始了飞速发展，国内网民群体的大量出现，为网吧行业再次提供了极大的发展与推动，连锁网吧的优越性在计算机设备购买更新、提供服务种类、经营管理手段方面具有一定的优势，与相关产业的结合度将更为紧密。

4. 现状

根据 CNNIC《第 29 次中国互联网络发展状况统计报告》显示：截至 2011 年底，中国网民人数已经达到 5.13 亿人，在网吧上网的网民占网民总数的 27.9%，较 2010 年下降 7.8%，首度出现负增长。

据文化部《2011 中国网吧市场年度报告》显示，截至 2011 年底，全国共有网吧 14.6 万家。其中，经认定的全国网吧连锁企业 4 家，省级连锁企业 232 家，区域性连锁企业 343 家。网吧终端台数 1152 万台，从业人员 107 万人，各级网吧协会 922 个，“五老”义务监督员近 14 万人。从市场占有率看，目前全国网吧连锁率已接近 40%。

2006 年之后，有些网吧特别是大城市网吧的发展开始从单一走向多模式的发展。例如某些大型网吧已经不是传统意义上的单纯网吧营业，在这些网吧旁边还有配套的茶吧、酒吧及其他娱乐休闲类场所，从某种意义上来说这些网吧已经形成了具有自己独特的网吧文化，已经脱离了“上网、玩游戏”的单调经营理念。

5.1.2　互联网上网服务营业场所的安全问题

随着网吧行业的发展，也衍生出很多问题，违规经营、秩序混乱、安全隐患突出，网瘾尤其是网络中黄赌毒的危害已经严重影响人们的生活学习，毒害人们的身心健康，尤其增大了青少年的犯罪率，严重影响社会治安和社会风气。网吧已成为社会热点问题、焦点问题，必须引起高度重视。

1. 信息网络安全问题

互联网上充斥着大量不健康的有害信息，淫秽、色情信息严重损害了人们的身心健康。有些人利用网吧做掩护，通过网上联络、非法交易，从事卖淫嫖娼、网络赌博等非法活动。一部分人无视法律、法规的规定，制作、复制、传播各种造谣、污蔑、诽谤他人的信息和言论，肆意散布谣言，蛊惑人心，歪曲事实，以发泄对社会制度的不满情绪，严重破坏安定团结的和平

局面。还有一些上网消费者在网吧中散布木马等恶意程序，窃取银行、邮箱、网游等账号密码，侵犯公民财产权、隐私权。更有甚者，利用计算机病毒恶意入侵、攻击、破坏其他网络，破坏网络秩序，危害网络安全，直接影响社会的稳定和发展。

据统计，60%以上的网络案件源自网吧，不法分子以网吧为载体，实施各类网络违法犯罪；但由于网吧日志留存不健全，导致难以追查。由此可见，信息网络的安全直接影响到整个社会和谐稳定的大局。

2. 治安问题

网吧已经成为社会治安问题的高发场所之一。由于网吧是流动人口较集中的场所，环境复杂、人员素质差距大，会出现一些青少年因琐事打架斗殴。

上网的青少年由于其自身没有经济来源，为了筹钱上网，有些偷家里的钱物，有些盗窃、抢劫他人财物，甚至误伤他人。一些上网消费者专注于网络游戏或信息，忽视了对财物的保管，给违法犯罪人员带来了可乘之机。

除此之外，还有人利用网络可以不见面参与交易和上网地点可转移的特点从事种种非法的交易；有人通过在网上发布“帖子”侮辱、诽谤他人；有人把电子邮箱作为一种非常规作案的手段；更有甚者，有人把网吧当做违法犯罪后的藏身之处。

由此可见，进一步提升网吧治安管理水平，才能更好地规范网吧经营秩序、净化网吧治安环境。

3. 消防问题

随着网吧行业的发展，网吧规模不断扩大，网吧经营者在追逐经济效益的同时，忽视了网吧必要的安全防范。由于思想麻痹、疏忽大意，缺乏有效的安全监管，使网吧的安全隐患日趋严重。近年来，连续发生多起网吧重、特大消防事故。2002 年北京“蓝极速”网吧发生大火，网吧无任何消防措施，大门锁死，窗户被焊死，致 25 人死亡。2006 年河南省平顶山市“皓月网吧”发生火灾，致 1 死 26 伤，其中大部分为未成年人。2011 年浙江省象山县石浦镇“天一网吧”发生火灾，致 2 人死亡。2012 年山西省朔州市马邑路“育人网络”突发大火，所幸无人伤亡。

网吧存在的消防隐患，主要有以下几个方面：装修材料选择不当；选址偏僻，不利于救援；安全出口不足，通道被占用；电气线路超负荷、老化，耐火等级低；消防设施不达标；从业人员缺乏消防知识等。

“蓝极速”事件后，国家加大了对非法网吧的管理和处罚力度，在国家相关法律法规相继出台后，网吧发生火灾的次数和伤亡人数有所减少，但这并不代表没有火灾隐患，消防安全问题仍是重中之重。

4. 经营管理问题

网上聊天和网络游戏现在正成为对青少年特别是对中学生影响最大的网上因素。网络世界对于青少年具有强烈的诱惑力，不少人“网聊”成瘾，对“网游”执迷不悟，沉溺在虚拟的

世界中无法自拔，长期盯着计算机屏幕一动不动，不仅有损他们的身体健康，对他们的学习、情感和人生观的正确发展，都具有极大的负面影响。但有些网吧的经营者为了吸引并揽住那些上网的青少年，不仅提供饮料、零食、香烟以及泡好的方便面，还有专门的厨房为他们提供盒饭，甚至还为那些彻夜上网不回家的人提供毛毯。

还有一些上网消费者特别是年轻人经常浏览一些不健康的有害信息，而许多网吧为招揽生意对浏览黄色网站的行为熟视无睹，还专门设立“单间”满足消费者的“需求”。

在网吧的经营过程中，一些网吧为了减少成本，提高经济效益，忽视管理，其具体表现在：一是未成年人在网吧上网的情况屡禁不绝。不同程度地存在使用临时卡和公用卡现象；二是很多网吧不认真落实实名制登记，一旦发生网络违法犯罪案件，给公安机关调查取证造成了很大困难；三是不少网吧为贪图便利，通过使用身份证生成器或者他人身份信息办理临时卡登记手续。如此一来，一旦出现违法犯罪，身份信息被冒用者的权益就受到了侵害。

由于网吧经营者缺乏良好服务的经营理念，加上网吧管理员未能履行职责，很少进行巡查，对上网消费者的上网行为放任自流，使网吧成为不良网络内容滋生、泛滥的温床和不良网络行为的传播地。

5. 黑网吧问题

尽管国家出台相关法规，加大对网吧的监管管理。然而，中国的网吧业发展有其自身的特殊之处，即长期存在着大量的“黑网吧”。

关于“黑网吧”，并没有一个准确权威的定义。从狭义上来讲，“黑网吧”仅指无照经营或证照不全的网吧；但从广义的角度来讲，只要是违法经营的网吧就不是合法网吧，概括起来主要包含以下几种情形：一是无照经营或证照不全的网吧；二是接纳未成年人的网吧；三是装有非网络游戏的网吧；四是有浏览黄色信息或反动信息记录的网吧；五是通宵营业的网吧。

目前，“黑网吧”已由城镇向农村、城乡结合部和高校园区附近转移，形式上也由公开向隐蔽、由门店经营向家庭经营转化。这些“黑网吧”为逃避监管，隐藏在学校及居民区周边，低价吸引上网消费者，偷逃税收违法经营。由于国家 2007 年即停止新网吧的经营审批，此类“黑网吧”无法申请执照就得不到执法部门的有效监管。“黑网吧”一般条件简陋，经营场地狭窄、脏乱，空气污浊，通风不良，缺乏起码的消防设施，经营期间经常锁上安全门，堵塞安全通道，安全隐患让人忧心。这些“黑网吧”存在成本低利润高的现象，网吧经营者为了牟取暴利不惜违规操作。“黑网吧”的存在，对于网吧的整体形象以及连锁网吧的发展都带来不同程度的影响，有损良性的竞争秩序。这些问题的存在，严重地危害了社会秩序和经济秩序。

5.2 互联网上网服务营业场所安全管理

5.2.1 管理依据

1.《互联网上网服务营业场所管理条例》

为了满足网民通过网吧上网的巨大需求，同时对管理混乱、经营无序、事故不断的网吧进行监管，国务院于2002年9月29日公布了《互联网上网服务营业场所管理条例》（以下简称《条例》），该条例自2002年11月15日起施行。《条例》是我国互联网管理领域的一项重要法规，为加强对互联网上网服务营业场所的管理，提供了较高效力层次的法制依据和重要的法制保障。该《条例》自施行以来，对于加强网吧的管理，规范经营者的经营行为，维护公众和经营者的合法权益，保障互联网上网服务经营活动健康发展，促进社会主义精神文明建设发挥了重要的作用。

（1）内容

在《条例》中，明确规定了互联网上网服务营业场所的定义、职能分工、设立程序及条件、经营管理、安全管理、消防管理、治安管理和处罚等内容。

该《条例》主要针对互联网上网服务营业场所进行管理，是有关行政管理机关对互联网上网服务营业场所进行监督、指导和违法处罚的主要法律依据，也是互联网上网服务营业场所经营单位守法经营、加强互联网上网服务营业场所内部经营管理的重要法律依据之一。《条例》中规定，"互联网上网服务营业场所经营单位应当遵守有关法律、法规的规定，加强行业自律，自觉接受政府有关部门依法实施的监督管理，为上网消费者提供良好的服务。"

（2）规定的禁止行为

《条例》对经营单位规定了一些禁止行为：

① 禁止接纳未成年人进入互联网上网服务营业场所的行为。

② 禁止利用互联网上网服务营业场所进行赌博和变相赌博的行为。

③ 禁止擅自停止实施安全技术措施的行为。

④ 禁止利用互联网上网服务营业场所制作、下载、复制、查阅、发布、传播国家法律、法规所禁止的有害信息的行为。

⑤ 禁止在互联网上网服务营业场所内从事破坏网络安全的各种行为。

⑥ 禁止明火照明和吸烟，严禁带入和存放易燃、易爆物品；不得安装固定的封闭门窗栅栏。

⑦ 营业时间禁止封堵或锁闭门窗、安全疏散通道和安全出口。

2. 其他相关法律规范

（1）《中华人民共和国刑法》。

1997年《中华人民共和国刑法》修改后，除了分则规定的大部分犯罪罪名（包括危害国

家安全罪，危害公共安全罪，破坏社会主义市场经济秩序罪，侵犯公民人身权利、民主权利罪，侵犯财产罪，妨害社会管理秩序罪）都适用于利用计算机网络实施的犯罪以外，还专门在第二百八十五条和第二百八十六条分别规定了非法入侵计算机信息系统罪、破坏计算机信息系统罪两种针对计算机信息系统实施的专门犯罪。第二百八十七条规定了利用计算机实施犯罪的处罚。

(2)《中华人民共和国治安管理处罚法》。

2005 年 8 月 28 日，第十届全国人民代表大会常务委员会第十七次会议通过了《中华人民共和国治安管理处罚法》，自 2006 年 3 月 1 日起施行。增加了信息网络领域违法行为的相关条款，对利用互联网实施扰乱社会治安管理的违法行为做了明确规定，为公安机关网络安全保卫部门在信息网络领域维护社会秩序，保证公共安全，保护公民、法人和其他组织的合法权益提供了有力的法律依据和重要的法律武器。其中，第二十五条、第二十七条、第二十九条、第四十二条、第四十七条、第四十九条、第五十四条、第五十五条、第六十八条、第六十九条和第七十条等部分条款着力体现了《中华人民共和国治安管理处罚法》对信息网络领域违法行为的规范。

(3)《计算机信息网络国际联网安全保护管理办法》。

1997 年 12 月 16 日公安部发布了《计算机信息网络国际联网安全保护管理办法》。这是我国第一部全面调整互联网络安全的行政法规，不仅对我国互联网的初期发展起到了重要的保障作用，而且为后续有关信息安全的法规、规章的出台起到了重要的指导作用。该《办法》第三条规定“公安部计算机管理监察机构负责计算机信息网络国际联网的安全保护管理工作”。

(4) 近几年来，国家政府各主要行政部门几乎每年都要针对网吧联合下发通知，对网吧行业的发展和监管做出具体要求，这些规章和要求既有针对性，又有着很强的连贯性，不仅体现了党和国家对网吧行业发展的高度关注和重视，也在实践工作中为网吧行业的健康、繁荣发展起到了积极的指导和促进作用。

2003 年 5 月 10 日，文化部以第 27 号令发布了《互联网文化管理暂行规定》(后于 2004 年 7 月 1 日以第 32 号令进行了修订)；2004 年 2 月 17 日，国务院办公厅转发了文化部等部门《关于开展网吧等互联网上网服务营业场所专项整治意见的通知》(国办发[2004]19 号)；同年 10 月 18 日，文化部、工商总局等九部委联合发布了《关于进一步深化网吧专项整治工作的意见》(文市发[2004]38 号)，要求有关部门继续深入开展网吧专项整治行动；2005 年 5 月 26 日，文化部、工商行政总局等九部委联合下发了《关于进一步深化网吧管理工作的通知》(文市发[2005]104 号)；2007 年 2 月 15 日，文化部、工商总局等 14 个部门联合印发了《关于进一步加强网吧及网络游戏管理工作的通知》(文市发[2007]104 号)；2008 年 7 月 7 日，文化部、国家工商行政管理总局、公安部联合下发了《关于网吧管理工作有关问题的通知》(文市发[2008]25 号)；2009 年 9 月 7 日，文化部印发了《网吧连锁企业认定管理办法》(文市发[2009]35 号)；2011 年 10 月，新闻出版总署等八部门联合印发《关于启动网络游戏

防沉迷实名验证工作的通知》，网络游戏防沉迷实名验证于 10 月 1 日起在全国范围内正式实施。

5.2.2 管理职能

加强网吧监管，是构建社会主义和谐社会的客观需要。进一步整顿和规范网吧经营秩序，需要多方位、多层次的管理模式，它涉及政府的多个职能部门、网吧经营单位及上网消费者。具体来说，网吧的安全管理包含四个层面的管理。

1. 政府职能部门应依法对互联网上网服务营业场所经营单位行使有效的监督、检查和管理

互联网上网服务营业场所的监督和管理，由多个政府部门共同负责，这主要是为了相互监督和制约。针对网吧中存在的各种现实问题和突出问题，各地的公安机关、文化行政部门、工商行政管理部门、互联网运营服务商要根据《互联网上网服务营业场所管理条例》的规定，制定出具体的政策，采取切实可行的措施，齐抓共管，将网吧安全管理中存在的问题减小到最低程度，努力营造良好的上网环境。

1）公安机关安全监管职责

《互联网上网服务营业场所管理条例》中第四条规定“公安机关负责对互联网上网服务营业场所经营单位的信息网络安全、治安及消防安全的监督管理”。

公安机关管理网吧的主要职责是：依法对网吧进行信息网络安全和消防安全审核；指导、督促网吧建立健全安全管理制度，落实上网实名登记等安全技术措施；依法对网吧信息安全、治安秩序、消防安全进行检查；依法查处网吧违反信息安全、治安和消防等法律法规的行为。公安机关网络安全保卫部门、消防部门、派出所实行三位一体安全防范管理模式。

（1）信息网络安全监督管理。

信息网络安全监督管理是互联网上网服务营业场所安全管理的重要组成部分，由公安机关网络安全保卫部门负责，具体职责为：

① 监督、检查、指导互联网上网服务营业场所信息网络安全保护工作。

② 组织实施互联网上网服务营业场所信息网络安全评估、审核。

③ 查处互联网上网服务营业场所发生的计算机及网上违法犯罪案件。

④ 落实互联网上网服务营业场所各项安全制度和安全技术措施的实施工作。

⑤ 组织处置重大互联网上网服务营业场所信息网络安全事故和事件。

⑥ 负责计算机病毒和其他有害数据防治管理工作。

⑦ 对互联网上网服务营业场所信息网络安全服务和安全专用产品实施管理。

⑧ 负责互联网上网服务营业场所信息网络安全培训管理工作。

⑨ 履行法律、法规所赋予的安全保卫工作的其他监督职能。

（2）治安监督管理。

基层派出所要加强对互联网上网服务营业场所的安全巡查，进一步细化、落实安全防范措施，切实加强互联网上网服务营业场所等公众聚集场所的治安防范工作，确保人民群众生命、财产安全。具体职责为：

① 负责互联网上网服务营业场所的治安管理工作。

② 抓好互联网上网服务营业场所内部的治安防范。

③ 负责查处或侦破互联网上网服务营业场所发生的行政案件、刑事案件。

④ 履行法律、法规所赋予的其他职能。

（3）消防监督管理。

针对互联网上网服务营业场所内人员流动性大、消防隐患突出的问题，公安消防部门要严格互联网上网服务营业场所的消防安全审核和安全检查，切实解决互联网上网服务营业场所中存在的消防安全措施不落实、消防通道不畅等问题，及时消除安全隐患。具体职责为：

① 监督、检查、指导互联网上网服务营业场所消防安全措施的落实。

② 负责互联网上网服务营业场所消防安全进行审核。

③ 依法查处违反国家消防安全规定的违法行为。

④ 履行法律、法规所赋予的其他职能。

2）文化行政部门管理职责

（1）负责互联网上网服务营业场所经营单位的设立审批。

（2）负责对依法设立的互联网上网服务营业场所经营单位经营活动的监督管理。

（3）宣传《互联网上网服务营业场所管理条例》及相关法律、法规。

3）工商行政管理部门管理职责

（1）负责对互联网上网服务营业场所经营单位登记注册和营业执照的管理。

（2）负责依法查处无照经营、超范围经营活动。

（3）对互联网上网服务营业场所的日常监督管理。

4）其他部门管理职责

互联网运营服务部门主要负责对上网服务营业场所互联网接入服务与监管，对应当停止接入服务的网吧停止接入服务，对违法提供接入服务行为进行查处。

教育行政部门负责加强对学校内互联网上网服务营业场所的治理，要求各级各类学校加大对未成年人不得进入网吧的宣传教育和管理力度，严格校纪校规，提倡利用现有的计算机网络资源，为学生正常学习提供必要的上网条件。

各级政府的精神文明办公室负责加强对网吧等互联网上网服务营业场所不同时期专项整治工作及有关法律法规的学习与宣传。

共青团组织应当广泛宣传《全国青少年网络文明公约》，引导未成年人增强自我保护意识，加强自我管理，自觉远离网吧。

2. 互联网上网服务营业场所经营单位及从业人员应加强法律、法规意识，严格守法经营

互联网上网服务营业场所的安全管理仅仅依靠政府职能部门的监管是远远不够的，应该在加大政府监管力度的同时，努力提高互联网上网服务营业场所经营单位的社会责任意识，注重和加强行业自律，加强互联网上网服务营业场所行业内的交流与沟通，不断提高互联网上网服务营业场所经营单位和从业人员的自身素质、管理水平和服务意识，努力成为文明上网场所的提供者和互联网高科技知识推广普及的宣传者。具体体现在以下几个方面：

(1) 接受公安机关的监督、检查和指导。

(2) 严格制定、完善、执行各项安全管理制度和安全预案，责任落实到人。

(3) 采取必要的安全技术保护措施，确保各项安全管理系统正常运行。

(4) 配备相应计算机设备和网络安全管理技术人员，定期对管理人员进行培训。

(5) 正确引导上网消费者的上网行为。

(6) 确保经营场所符合消防安全条件，安全设施齐全。

(7) 加强互联网上网服务营业场所内治安和安全巡查，发现有网络或其他违法犯罪行为应立即制止并及时上报有关部门。

(8) 法律、法规对经营单位规定的其他责任。

3. 上网消费者应严格遵守国家有关法律、法规的规定，文明上网

上网消费者作为互联网上网服务营业场所管理的重要组成部分，应该严格遵守国家的各项法律、法规和有关政策，提高自身文化素质，做到文明上网，不助长谣言传播。树立正确的消费目的和消费观念，把单纯的网上娱乐逐步转变为获取知识、学习交流。积极主动地配合互联网上网服务营业场所各项制度的执行和安全管理，不从事违反国家法律、法规的活动和行为。具体体现在以下几个方面：

(1) 认真履行上网审核的实名登记制度和上网登记制度。

(2) 不制作、复制、传播、浏览国家法律、法规所禁止的各类信息，净化网络信息，营造健康、文明的网络环境。

(3) 不从事国家法律、法规所禁止的各种破坏信息网络安全的活动，共同创造和维护安全、可靠的网络环境。

(4) 不侵犯、占有他人的网络资源和虚拟财产，保护网络用户的通信秘密和通信自由。

(5) 法律、法规对上网用户规定的其他责任。

4. 建立广泛的社会监督机制及长效管理机制

互联网上网服务营业场所安全一直是管理工作的重点、社会反映的热点，也是日常管理的难点，对互联网上网服务营业场所的管理稍有松懈就会出问题。因此，在加强社会监管的基础上，还要建立一整套完善的长效机制。把切实加强互联网上网服务营业场所管理作为维护广大人民群众利益、保障未成年人健康成长的一件大事，抓紧抓好，抓出

成效。建立的管理机制主要包括：

1）社会监管工作机制

进一步完善社会监督、舆论监督和执法监督体系，强化互联网上网服务营业场所监管力度。文化主管部门要聘请人大代表、政协委员、离退休老干部、教师和学生家长等社会不同层面人员成立互联网上网服务营业场所义务监督队，颁发监管证，开展经常性的监督活动。新闻媒体要加大明察暗访力度，对违规行为和处罚结果要定期在媒体上予以曝光，接受社会监督。纪检监察部门要加大对文化、公安、工商、电信等部门和其他有关部门及其工作人员参与或变相参与互联网上网服务营业场所经营活动和为互联网上网服务营业场所违法经营活动营私舞弊行为的查处力度。

2）投诉举报工作机制

通过各种方式鼓励社会各界人士对互联网上网服务营业场所经营活动中的违法违规经营行为及时举报，形成全社会共同关心文化市场经营和管理的舆论氛围。要公布所有互联网上网服务营业场所，设立举报电话、举报信箱，建立必要的奖励制度。

3）宣传教育工作机制

宣传、教育部门要充分发动学校、家长以及社会各界共同担负起帮助教育青少年的社会责任，在中小学校开展各种形式的专题教育，积极倡导文明上网。文化、新闻等管理部门要利用各种媒体、载体宣传相关法律、法规，让上网消费者真正地了解到网吧安全管理的法律、法规和各项安全管理制度。

4）联合执法工作机制

各有关部门要加强协调配合，形成分工负责、整体联动的工作格局。紧紧抓住校园周边环境整治等社会热点，公安、文化、工商等部门建立健全执法协作、信息共享等工作机制，明确各自职责分工、协作内容和联动方式等事项，建立查处“黑网吧”等重大案件执法预案，实现综合治理。

5.2.3　互联网上网服务营业场所信息网络安全管理

信息网络安全管理是互联网上网服务营业场所安全管理的重要组成部分，因此，加强互联网上网服务营业场所的信息安全管理尤为重要。

1. 互联网上网服务营业场所信息网络安全管理制度

随着互联网信息的飞速发展，网上黄、赌、毒的现象日益突出，不断侵蚀着上网消费者尤其是青少年的思想，网络违法犯罪案件不断增加。为进一步规范互联网上网服务营业场所的管理工作，营造绿色的上网环境，建立一套行之有效的信息网络安全管理制度势在必行。管理制度的建立健全，是互联网上网服务营业场所安全管理的保障，能有效预防各种网上违法犯罪活动的发生，对维护互联网上网服务营业场所正常的经营秩序有着重要意义。

1）上网审核登记制度

互联网上网服务营业场所的上网审核登记制度是确保上网人员合法身份的安全管理制度，也是网络实名化的体现。

《互联网上网服务营业场所管理条例》第二十三条规定："互联网上网服务营业场所经营单位应当对上网消费者的身份证等有效证件进行核对、登记，并记录有关上网信息"。

早期，多数互联网上网服务营业场所安全管理人员主要采用口头询问、检查、记录的方式，虚假登记或不登记等情况比较普遍，给网吧安全管理工作带来很大难度；之后，全典公司提出"网吧实名制管理"方式，即在上网登记的管理基础上，依托于IC卡管理模式，借助管理软件，建立公安监控与网吧经营之间的实时联系，让登记资料处于有效的监控状态，便于非法访问者的追查以及青少年上网的控制。

虽然上网登记卡与身份证信息挂钩，但上网时须同时出示身份证和上网登记卡，比较麻烦；开户或者补办上网登记卡都需要一定的费用；少数网吧经营者对上网登记卡管理不严，借用他人上网登记卡上网或使用假身份证上网的现象时有发生，使实名制执行不够彻底。

针对这些问题，网吧身份证刷卡实名制相继在各地实施。目前，直接用二代身份证刷卡上网，身份证中包含的图文信息直接在网吧管理员的计算机上显示，管理员可以清晰核对上网消费者的相关信息，方便、快捷、准确。

在互联网上网服务营业场所实行上网审核登记制度不仅对杜绝未成年人进入网吧上网有一定的保障作用，而且为公安机关对互联网开展公开管理、打击网络犯罪和案件侦破等工作提供有力保障，并将对净化网络环境起到良好作用。

2）上网信息记录留存制度

上网信息记录留存制度是对上网消费者的网络行为进行登记的管理制度。上网信息是指计算机操作系统或其安全技术措施以电子数据形式所记录的上网操作过程，包括上网消费者身份记录、上下网时间及系统运行日志记录。

《互联网上网服务营业场所管理条例》第二十三条规定："互联网上网服务营业场所经营单位应当对上网消费者的身份证等有效证件进行核对、登记，并记录有关上网信息。登记内容和记录备份保存时间不得少于60日，并在文化行政部门、公安机关依法查询时予以提供。登记内容和记录备份在保存期内不得修改或者删除。"

认真制定、执行上网登记制度并准确地记录上网消费者的上网信息，可以对上网消费者进入互联网的行为进行有效监督和控制，在发生网络违法案件时，也可以通过留存的上网信息进行跟踪、分析，从中获取违法犯罪的相关证据，对维护国家的信息网络安全、打击违法犯罪具有重大意义。

3）场内巡查与情况报告制度

互联网上网服务营业场所场内巡查与情况报告制度是为维护互联网上网服务营业场所安全、信息网络安全及在巡查中发现违法犯罪行为时及时予以制止和报告而制定的安全管理制度。

《互联网上网服务营业场所管理条例》第十九条规定："互联网上网服务营业场所经营单位应当实施经营管理技术措施，建立场内巡查制度，发现上网消费者有本条例第十四条、第十五条、第十八条所列行为或者有其他违法行为的，应当立即予以制止并向文化行政部门、公安机关举报"。

网吧要建立完善的场内巡查与情况报告制度，首先要配备足够的网络专业技术人员及管理人员，要求持证上岗，在各自的巡查区域内不间断进行巡查，并做好巡查记录；巡查员要正确引导上网消费者的上网行为，巡查时若发现上网消费者有登录非法网站，制作、下载、复制、查阅、发布、传播有害和违法的信息，危害信息网络安全，利用网络游戏或者其他方式进行赌博或者变相赌博活动，浏览色情网站等违法行为的，应当立即采取劝阻、口头警告、停止其上网等措施予以制止，并立即向文化行政部门、公安机关报告，并积极提供有关日志资料和有关信息协助公安机关进行查处。

执行场内巡查与情况报告制度对维护场所内的信息安全、正常经营秩序，预防突发事件是非常必要的。

4）变更备案制度

变更备案制度是指当互联网上网服务营业场所变更名称、地址、法定代表人或者主要负责人、注册资本、网络地址（IP）、IC 卡收费系统，扩大营业面积，改变上网计算机数量或者终止经营活动等情况时，根据《互联网上网服务营业场所管理条例》第十三条规定，应当经原审核机关同意。

互联网上网服务营业场所经营单位变更营业场所地址或者对营业场所进行改建、扩建，变更计算机数量或者其他重要事项，应当符合设立互联网上网服务营业场所的许可条件；互联网上网服务营业场所经营单位办理变更法定代表人登记事项的，按照 2009 年文化部《关于进一步净化网吧市场有关工作的通知》规定，应先注销其《网络文化经营许可证》后，按新设立互联网上网服务营业场所的标准和条件重新申请。

变更备案制度有利于公安机关、文化部门、工商行政部门等国家职能部门掌握互联网上网服务营业场所经营单位的相关信息，便于管理和监督。

5）信息安全培训制度

信息安全培训制度是指网吧的从业人员必须接受相应的信息安全培训，参加公安、人事部门联合组织的统一考试，考试合格后持证上岗。

根据《互联网上网服务营业场所管理条例》第八条规定，设立互联网上网服务营业场所经营单位，应具备与其经营活动相适应并取得从业资格的安全管理人员、经营管理人员、专业技术人员。公安机关要求新开办的网吧必须有两名以上取得培训合格证的安全管理人

员、专业技术人员。

培训的目的在于提高互联网上网服务营业场所从业人员的计算机网络安全知识、计算机病毒及防治知识、计算机安全法律法规知识，以此提高互联网上网服务营业场所自身的网络安全防范能力，保持互联网上网服务营业场所安全管理软件的正常运行、使用和更新，防范和制止网络犯罪、安全事故的发生。

2. 互联网上网服务营业场所信息网络安全管理技术措施

为加强和规范互联网安全技术防范工作，保障互联网网络安全和信息安全，促进互联网健康、有序发展，维护国家安全、社会秩序和公共利益，根据《计算机信息网络国际联网安全保护管理办法》，2005 年 11 月 23 日公安部发布了《互联网安全保护技术措施规定》。

互联网上网服务营业场所安全保护技术措施是指保障互联网网络安全和信息安全、防范违法犯罪的技术设施和技术方法。落实相关的信息网络安全管理技术措施，是对落实安全管理制度的进一步深化，是互联网上网服务营业场所的网络安全管理和保护网络安全必要的技术保障，对降低政府的网吧管理成本、提高管理效率起到积极作用。

互联网上网服务营业场所经营单位负责落实网吧的安全保护技术措施，并保障网吧的安全保护技术措施功能的正常发挥；公安机关网络安全保卫部门负责对网吧的安全保护技术措施的落实情况依法实施监督管理。

目前在网吧中实施的安全技术措施主要有：安装实名登记系统和安全管理系统；根据公安机关的部署安装视频监控系统；安装相关技术系统与公安机关管理平台实现联网运行；防范计算机病毒、网络入侵和攻击破坏等危害网络安全事项或者行为的技术措施；记录并留存用户登录和退出时间、主叫号码、账号、互联网地址或域名、系统维护日志的技术措施等。

5.2.4 互联网上网服务营业场所治安安全管理

2005 年 8 月 28 日通过的《中华人民共和国治安管理处罚法》，目的在于维护社会治安秩序，保障公共安全，保护公民、法人和其他组织的合法权益，规范和保障公安机关及其人民警察、依法履行治安管理职责。《中华人民共和国治安管理处罚法》中增加和调整了违反治安管理的行为和种类，规范了处罚程序，为保护群众合法权益提供了更有力的法律保障。

违反《中华人民共和国治安管理处罚法》所引起的责任是一种行政责任，但如果对受害方的人身或财产造成损失，则有可能引起民事损害赔偿，要依法承担民事责任。

1.《中华人民共和国治安管理处罚法》中规定的与网吧治安管理较密切的行为

（1）扰乱公共秩序的行为。

包括扰乱公共场所秩序行为；寻衅滋事行为；非法侵入、破坏计算机信息系统行为。

(2) 妨害公共安全的行为。

(3) 侵犯人身权利、财产权利的行为。

它包括威胁他人人身安全、侮辱诽谤、诬告陷害行为,妨害证人及其近亲属行为,传播骚扰信息行为,偷窥、偷拍、窃听、散布他人隐私行为;殴打、故意伤害他人身体行为;煽动民族仇恨、民族歧视行为;侵犯财产权利行为。

(4) 妨害社会管理的行为。

它包括妨害公务行为;非法经营行为;制作、运输、复制、出售、出租、传播淫秽物品、信息行为;赌博行为。

2. 网吧治安安全管理措施

为进一步提高网吧内部治安防控能力,规范网吧管理,维护上网消费者和经营者的合法权益,应该从建立长效机制出发,深化网吧监管服务,引导网吧健康、有序发展。具体的管理措施如下:

(1) 组织深入摸排,完善两级备案制度。组织派出所对辖区内的所有网吧进行彻底摸排,翔实登记,实现派出所、治安管理部门两级备案制度,对网吧的名称、地址、法定代表人、从业人员、经营管理情况进行登记。

(2) 开展集中整治,消除治安安全隐患。为彻底消除网吧内治安安全隐患,开展网吧集中治安整治行动,将群众反映强烈、容易造成人员聚集、存在消防安全隐患的网吧列为重点检查对象,及时发现、消除安全隐患,减少安全事故和案事件的发生。

(3) 加大从业人员培训,提高安全责任意识。对网吧管理人员进行网络安全管理、巡视工作制度、可疑报警等业务培训,提高他们的法律和安全意识,使他们能够真正担负起安全管理责任,定期检查安全设施,发现可疑的人事物及时向公安机关报告。

(4) 加强分工协作,建立管理长效机制。第一,明确治安、派出所等部门责任,加强沟通协作。组织开展经常性联合执法检查,坚持共同治理、标本兼治,形成齐抓共管的工作合力。第二,加强周边巡逻。派出所在日常巡逻时,有重点地加强网吧周边地区巡逻,预防和制止盗窃、寻衅滋事、两抢等案件的发生。第三,加大管理的科技含量。在网吧内推广安装视频监控系统,对网吧内部和周边情况进行动态监控,一方面对违法犯罪分子起到震慑作用,另一方面,加大对隐匿在网吧的违法犯罪人员的查控,也为侦破发生在网吧内的各类案件提供依据。第四,严查违法违规经营。对存在安全隐患和安全制度不落实的网吧,责令限期整改和停业;从事违法犯罪活动的,从严从重处罚。

5.2.5　互联网上网服务营业场所消防安全管理

根据我国消防工作"预防为主、防消结合"的方针,火灾预防是消防工作的重点。消防法对加强消防安全管理,落实防火安全责任制,预防火灾事故,保护公民人身、财产和公共财产安全是十分必要的。

根据网吧火灾危险性的特点,要加强网吧安全经营,预防火灾事故的发生,应采取以下

防范措施。

1. 网吧的选址

网吧应远离散发有害气体或存放腐蚀品、易燃易爆化学物品的地方，也不宜设在低洼潮湿或靠近强电磁场、强振动源和强噪音源的地方。尽可能设在建筑物的三层或三层以下靠外墙部位，避免设置在袋形走道的两侧或尽端或设置在地下二层及二层以下。

2. 网吧的室内装修

网吧的耐火等级不应低于二级，面积不宜大于 300m^2，大于 300m^2 时，应增设自动灭火系统。网吧应采用不燃难燃材料进行装修，但装修应保留足够的安全出口数量。装修中需穿墙的电缆应套金属管，管内不能有接头，穿越墙处的缝隙应使用不燃材料进行封堵，防止“窜火”。

3. 网吧内的温度和湿度

网吧的温度应控制在 15℃～25℃之间，温度过高不仅会造成计算机系统的主要元件集成电路失灵，而且计算机散热风扇长时间工作，也可能引发火灾事故。网吧内的湿度应控制在 40%～60%，湿度过高，容易造成集成电路失效或者发生短路；湿度过低，可能产生静电，烧毁 MOS 器件。而且，带静电后容易吸附灰尘，形成漏电打火。网吧经营者应经常为计算机除尘，平时不用时，应当在停机半小时后盖上防尘布罩，防止灰尘进入计算机。

4. 良好的电气环境

网吧应选用符合要求的不间断电源，防止因电压波动、干扰对计算机造成危害。网吧经营者要对计算机做好工作接地和防雷接地。网吧内各类电气设备的安装和维修、线路改动和临时用线，都应当在营业后在停机状态下由合格电工严格按照国家有关标准和规程操作安装，交流线路走线不能和直流地线紧贴平行敷设。

5. 严格的日常消防管理和消防安全管理制度

网吧内不应存放腐蚀性物品和易燃易爆危险物品，检修时应避免使用易燃溶剂如汽油、香蕉水等。要及时劝阻顾客在网吧内吸烟，更不允许随意动用明火。网吧营业时要保障疏散通道和安全出口的畅通，停止营业后，应当及时切断电源，并组织人员仔细巡查。网吧经营者应严格按照《建筑灭火器配置设计规范》配备灭火器材，为电气火灾初期扑救做好必备基础条件。

6. 网吧经营者在经营中应做到

（1）购买计算机时应优先选购质量信得过的产品。

（2）网吧的电线配置应合理，须购置合格电线，应根据网吧的用电量合理选用导线容量，并穿管保护。

（3）网吧经营者应经过消防安全培训，会使用消防器材，会报火警，会扑灭初起火灾，会组织疏散人群。

（4）加强网吧消防安全管理，禁止乱扔烟头、私接电线，疏散门应保持畅通，设置消防安全标志，并定期组织维修。

公安消防部门发现火灾隐患，应当及时通知有关单位或者个人采取措施，限期消除隐患。真正做到以上几点，网吧就能够筑起一道难以攻破的防火墙，有效地预防火灾事故的发生。

5.3　互联网上网服务营业场所安全监管

公安机关对申请设立的网吧进行安全审核，包括安全管理制度和安全保护技术措施的建立健全。在督促网吧建立相关制度后，采取定期或不定期的方式对网吧进行检查，指导、督促网吧经营者落实相关制度。同时，每年在对网吧的安全审核中，都要认真核实网吧备案资料，对网吧情况有变动的，都要到现场进行实地查看，为搞好网上案件侦破工作奠定坚实的基础。

5.3.1　安全审核

《互联网上网服务营业场所管理条例》规定："申请人完成筹建后，持同意筹建的批准文件到同级公安机关申请信息网络安全和消防安全审核。"互联网上网服务营业场所安全审核包括网吧场所安全审核、网吧网络结构安全审核、网吧硬件系统安全审核、网吧互联网接入线路安全审核以及网吧消防安全审核。

1. 安全审核内容

根据公安部《关于加强互联网上网服务营业场所安全管理工作的通知》的规定，公安机关安全审核的主要内容有：

(1) 经营人员是否具有合法的身份证明。

(2) 营业场地是否符合消防安全的有关规定。

(3) 营业场地面积、计算机终端数量是否符合规定要求。

(4) 有无被撤销批准文件的记录。

(5) 有无专职的或兼职的安全管理人员。

(6) 有无相应的防病毒、防有害信息传播等安全技术措施。

(7) 有无经安全检测合格的互联网上网服务营业场所经营单位安全管理软件。

(8) 是否符合国家现行法律、法规的规定。

2. 安全审核需提交的材料

申请人在取得文化行政部门同意设立的核准文件后，应当向公安机关申请核发信息网络安全和消防安全审核批准文件，并提交以下材料：

(1) 文化行政部门同意筹建的批准文件。

(2) 消防安全审核意见书。

(3) 工商行政管理部门出具的名称预先核准通知书。

（4）自有营业场所产权证明或者租赁合同及业主产权证明。

（5）营业场所位置图、平面图；网络拓扑结构图（路由器型号、交换机数量和型号、机位号与内网 IP 对应表）。

（6）与互联网接入服务提供商签订的接入协议。

（7）实名身份认证系统安装证明。

（8）信息网络安全审计系统软（硬）件安装证明。

（9）视频监控联网系统安装证明。

（10）计算机通信设施防灾减灾系统安装证明。

（11）信息网络安全管理人员按照国家规定参加继续教育培训的证明材料。

3. 安全审核程序

县（市、区）公安机关消防机构和网络安全保卫部门对申请人的申请，应当自收到申请之日起 10 个工作日内进行实地检查，提出初审意见报地级以上市公安机关消防机构和网络安全保卫部门；地级以上市公安机关消防机构和网络安全保卫部门应当自收到初审意见之日起 10 个工作日内做出审查决定。审核合格的，发给批准文件；对审核不合格但依法可以整改的，应该通知申请人在规定的期限内整改，并重新报请审核，审核期限重新计算；对无法整改或经整改后仍不合格的，依法不予批准，并向申请人书面说明理由。

4. 安全审核管理要求

1）网吧场所安全审核

（1）网吧经营单位提供上网消费者使用的计算机必须通过局域网的方式接入互联网，不得直接接入互联网。

（2）上网场所必须采用固定的网络（IP）地址。

（3）上网场所应建立健全信息网络安全保护管理制度。

（4）上网场所必须建立网络安全小组，法定代表人及主要负责人、安全管理人员必须参加计算机安全员培训，经考试合格后发计算机信息网络安全员培训合格证书。

（5）上网场所的经营单位需提供所属网吧的网络结构拓扑图、内部 IP 对照表、室内平面布置图、营业场所实际地理位置图。

（6）上网场所需安装网络安全审计管理系统，上网场所的所有上网设备必须纳入安全审计系统。

（7）上网场所的经营单位需与公安机关签署网吧安全审计管理系统的安全保密协议。

（8）上网场所内提供上网服务的计算机必须是有盘工作站系统。

（9）上网场所需采取网络安全技术保护措施，防止计算机病毒、黑客软件等恶意程序对内部系统的破坏，同时不得擅自停止实施安全技术保护措施。

（10）上网场所必须严格落实上网人员实名身份登记制度，并按规定记录备份上网消费者的有关上网信息。

（11）上网场所需采取措施确保有关登记内容和记录备份的上网信息，保存时间不得少

于 60 日，在保存期内不得修改或者删除。

（12）上网场所必须配备 380V 三相四线电源。

（13）上网场所经营单位变更营业场所地址或者对营业场所进行改建、扩建，变更计算机数量或者其他重要事项的，应先提交书面申请，经同意后方可改变。

（14）上网场所经营单位和上网消费者不得利用互联网上网服务营业场所制作、下载、复制、查阅、发布、传播或者以其他方式使用有害信息。

2）网吧网络结构安全审核

针对目前公安网吧管理软件的技术标准，只有规范网吧的组网方式，才能充分发挥公安网吧管理软件的功能，便于公安机关有效监管网吧。一般要求网吧采用网管式交换机方式进行组网。网络拓扑如图 5-1 所示。

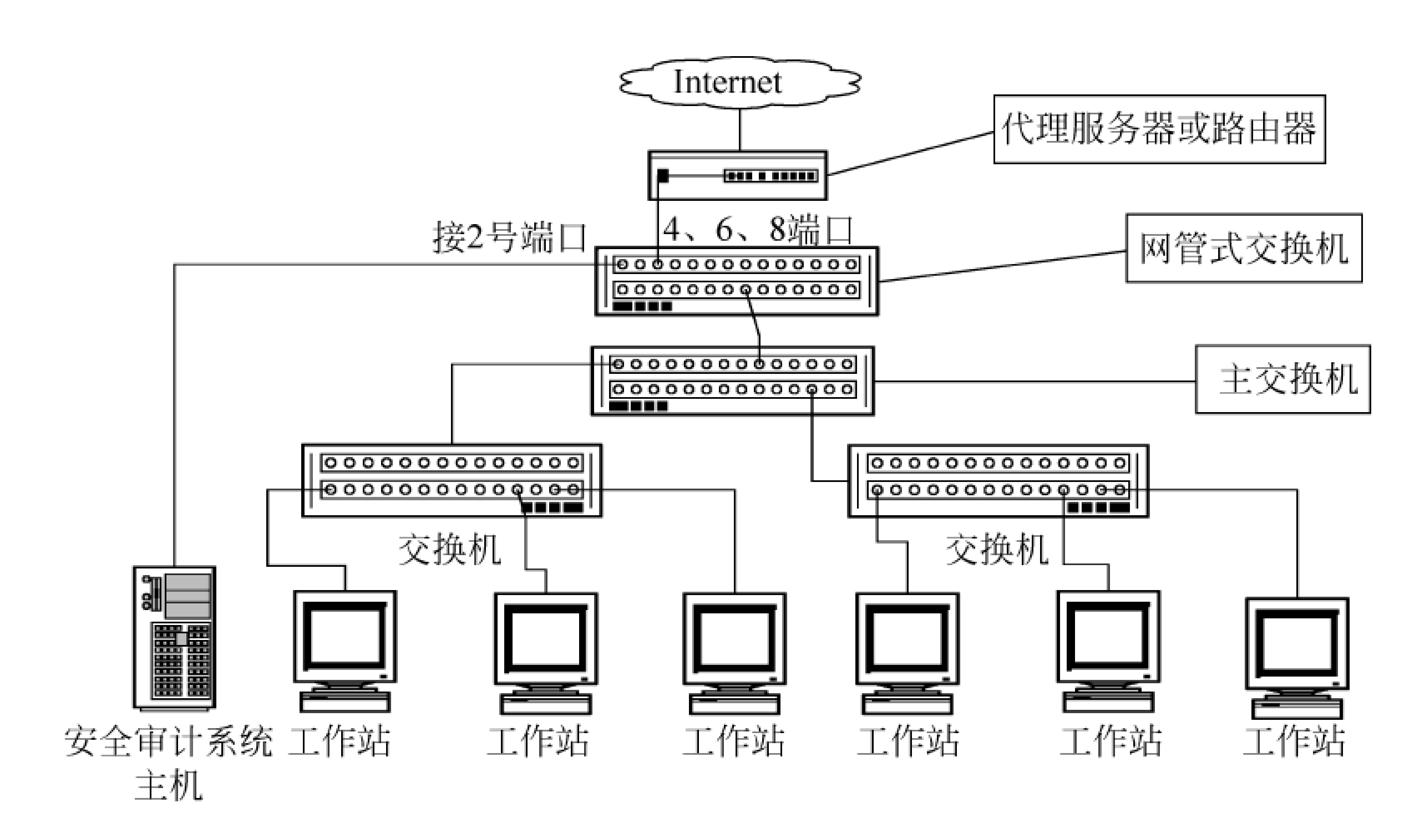


图 5-1　采用网管式交换机的网络拓扑图

3）网吧硬件系统安全审核

（1）审计机。网吧安装的安全审计技术产品必须采用经过公安部检测通过、具有计算机信息安全专用产品销售许可证的产品。安全审计系统和收费系统必须装在同一台主机上。

（2）连接设备是网管式交换机。

（3）上网计算机应是有盘工作站系统。

（4）工作站应分别指定 IP，不得采用自动获取的方式分配 IP。

4）网吧互联网接入线路安全审核

（1）互联网接入线路必须保证使用固定 IP。

（2）办理多条互联网接入线路必须向所在地公安机关网络安全保卫部门提出申请，经批准后安装使用。

(3) 每条接入线路应建立一套独立的安全审计系统和收费系统。即每一条固定 IP 为一个独立网段。

5) 网吧消防安全审核

(1) 互联网上网服务营业场所经营单位应当在法定代表人或者主要责任人中确定一名本单位的消防安全责任人。

(2) 互联网上网服务营业场所的安全出口数目、疏散宽度和距离,应当符合国家有关建筑设计防火规范的规定。安全出口处不得设置门槛、台阶,疏散门应当向外开启,不得采用卷帘门、转门、吊门或侧拉门,门口不得设置遮挡物。确保安全出口和疏散通道畅通。

(3) 安全出口、疏散通道和楼梯口应当设置符合标准的灯光疏散指示标志。

(4) 设置火灾事故应急照明灯,供电时间不得少于 20 分钟。

(5) 不得超负荷用电,不得擅自拉接临时电线。

(6) 禁止吸烟和明火照明。

(7) 互联网上网服务营业场所营业时,不得超过额定人数。

(8) 互联网上网服务营业场所经营单位应当制定防火安全管理制度,制定紧急安全疏散方案。

(9) 配置灭火器材,保证消防设施、设备完好有效。

(10) 内部装修设计和施工,应当符合《建筑内部装修设计防火规范》和有关建筑内部装饰装修防火管理的规定。

5.3.2 日常监管

2001 年 3 月 11 日公安部发布《公安派出所执法执勤工作规范》中规定,公安派出所"对行业、场所、单位的检查每月不得少于一次"。因此,把网吧纳入公安派出所的日常管理既有法律上的依据,又是网吧日常管理工作的需要。通过公安机关派出所、网络安全保卫部门、消防监督部门的日常检查,增加检查的密度,促使经营单位依法经营。

1. 现场检查

网吧日常监管主要以网吧现场检查为主。网吧现场检查工作流程如图 5-2 所示。

2. 消防监督检查

2004 年 9 月 1 日由公安部修改后正式实施的《消防监督检查规定》中规定,公安消防机构进行消防监督检查的形式主要是"对单位进行监督抽查",对消防安全重点单位的监督抽查每半年至少组织一次,对其他单位的监督抽查每年至少组织一次。

公安消防机构可以组织大范围的消防安全大检查,也可以结合某一时期的工作重点,针对当时消防安全存在的突出问题,开展专门性的消防监督检查活动。

消防监督检查的内容包括:

(1) 有关消防手续。

互联网上网服务营业场所在使用或开业前,必须有消防机构发给的《消防检查安全意

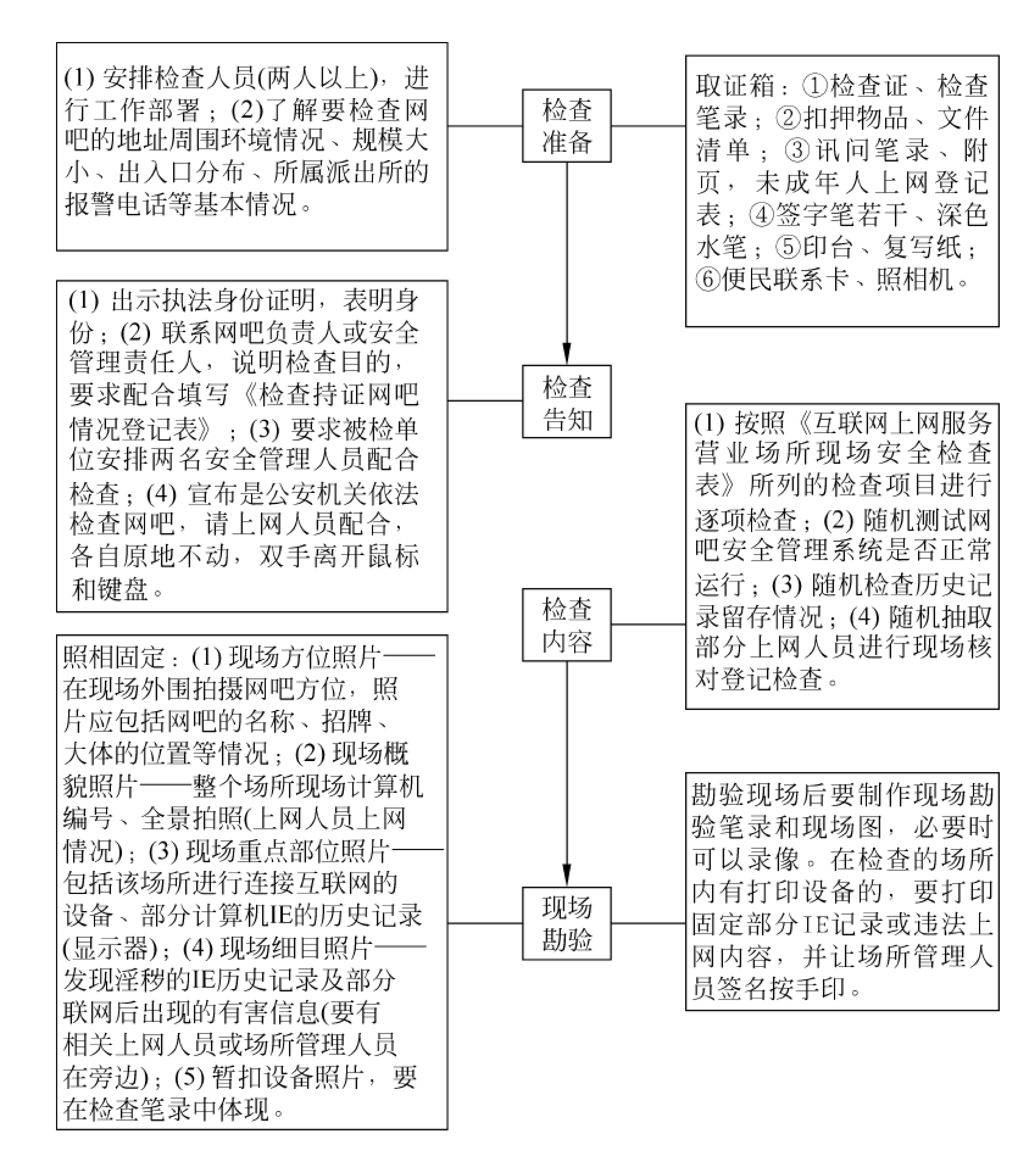


图 5-2　网吧现场检查工作流程

见书》。

(2) 已经通过消防设计审核和消防验收合格的下列项目的使用、改变情况：

① 总平面布局和平面布置中涉及消防安全的防火间距、消防车通道、消防水源等。

② 建筑物的火灾危险性类别和耐火等级。

③ 建筑防火、防烟分区和建筑构造。

④ 安全疏散通道和安全出口。

⑤ 防烟、排烟设施和通风、空调系统的防火设备。

⑥ 建筑内部装修防火材料。

⑦ 其他经消防设计审核、验收的内容。

(3) 消防安全管理的情况。

3. 相关表格

互联网上网服务营业场所申请登记表

编码□□□□□□□□□□状态□

<table>
<tr><td colspan="2">申请单位</td><td colspan="7"></td></tr>
<tr><td colspan="2">营业场所详细地址</td><td colspan="7"></td></tr>
<tr><td colspan="2">法定代表人姓名</td><td></td><td>身份证号</td><td colspan="5"></td></tr>
<tr><td colspan="2">联系电话</td><td></td><td>法人代码</td><td colspan="5"></td></tr>
<tr><td rowspan="4">网络情况</td><td rowspan="2">接入网络</td><td>名称</td><td colspan="3"></td><td>联系电话</td><td colspan="2"></td></tr>
<tr><td>地址</td><td colspan="6"></td></tr>
<tr><td>上网方式</td><td colspan="7">○拨号 ○ISDN ○ADSL ○DDN ○卫星
○帧中继 ○ATM ○X. 25 ○其他：________（请注明）</td></tr>
<tr><td>规模</td><td>服务器数量</td><td></td><td>终端数</td><td></td><td>营业面积</td><td colspan="2"></td></tr>
<tr><td rowspan="9">人员情况</td><td></td><td>姓名</td><td colspan="3">身份证号码</td><td>电话</td><td>专、兼职</td><td>培训状态</td></tr>
<tr><td>负责人</td><td></td><td colspan="3"></td><td></td><td></td><td></td></tr>
<tr><td rowspan="2">安全管理员</td><td></td><td colspan="3"></td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="3"></td><td></td><td></td><td></td></tr>
<tr><td rowspan="2">技术人员</td><td></td><td colspan="3"></td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="3"></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">经营人员数量</td><td colspan="6">其中专职人员：________人，兼职人员：________人</td></tr>
<tr><td rowspan="2">技术服务委托单位</td><td>名称</td><td colspan="3"></td><td>联系电话</td><td></td><td></td></tr>
<tr><td>地址</td><td colspan="6"></td></tr>
<tr><td colspan="2">安全措施及管理制度</td><td colspan="7"></td></tr>
<tr><td colspan="2">管理软件名称</td><td colspan="4"></td><td>检测证书号码</td><td colspan="2"></td></tr>
<tr><td colspan="2">开发单位</td><td colspan="7"></td></tr>
</table>

（以下由公安机关填写）

<table>
<tr><td colspan="2">县市级公安机关初审意见：

年　月　日
审核人签字：　（签　章）</td></tr>
<tr><td colspan="2">地市级公安机关审批意见：

年　月　日
审核人签字：　（签　章）</td></tr>
<tr><td>备
注</td><td>

×××公信安审字(　　　)号
年　月　日</td></tr>
</table>

互联网上网服务营业场所变更项目申请登记表

编码□□□□□□□□□□状态□

申请单位						
变更项目	○场所名称　○经营地址　○法人（负责人）　○接入单位　○上网方式 ○上网电脑台数　○技术人员　○安全管理员　○其他：					
变更理由	负责人签名： （申请单位签章）					
以下填写变更后的情况						
场所名称						
场所地址						
法人（负责人）姓名			身份证号			
联系电话			法人代码			
网络情况	接入网络	名称		联系电话		
		地址		固定 IP 范围		
	上网方式	○LAN　○ISDN　○ADSL　○DDN　○卫星 ○帧中继　○ATM　○VDSL　○其他：________（请注明）				
	规模	服务器数量		终端数		营业面积
人员情况		姓名	身份证号码	电话	专、兼职	培训状态
	负责人					
	安全管理员					
	技术人员					
	经营人员数量	其中专职人员：________人，兼职人员：________人				
安全措施及管理制度						
管理软件名称				检测证书号码		
网络版防病毒软件名称				销售许可证号码		

（以下由公安机关填写）

<table>
<tr><td rowspan="3">核
查
情
况</td><td>被取消联网资格或被暂停联网记录</td><td colspan="2"></td><td>管理制度是否上墙</td><td colspan="2"></td></tr>
<tr><td>网络地址是否固定并与申报的一致</td><td colspan="2"></td><td>终端数量</td><td colspan="2"></td></tr>
<tr><td>网吧安全管理软件安装情况</td><td></td><td>网络防病毒软件安装情况</td><td></td><td>核查人</td><td></td></tr>
<tr><td colspan="7">县（市、区）公安机关辖区派出所意见：

年　　月　　日
（签　章）</td></tr>
<tr><td colspan="7">县（市、区）公安机关公共信息网络安全保卫部门意见：

年　　月　　日
（签　章）</td></tr>
<tr><td colspan="7">县（市、区）公安机关审核意见：

年　　月　　日
审核人签字：　　（签　章）</td></tr>
<tr><td>备 注</td><td colspan="6">________公信安审字（　　　）号
年　　月　　日</td></tr>
</table>

互联网上网服务营业场所年审登记表

安全审核证书编号：

单位名称			
详细地址			
法定代表人		联系电话	
201____—201____年度年审记录 一、信息网络安全管理是否存在违规行为：是☐　否☐ 原因：________________ 二、信息网络安全管理系统、防病毒软件运行情况：正常☐　不正常☐ 原因：________________ 三、是否有足量的计算机安全员在岗并履行职责：是☐　否☐ 原因：________________ 年　月　日 审核人：　（盖县市级以上公安机关安全审核章）			

互联网上网服务营业场所从业人员登记表

填表时间：　年　月　日

1. 网吧申请负责人		身份证号			
现住地址					
传呼		手机		联系电话	
是否参加过计算机信息安全员培训并取得合格证					
个人工作简历					

续表

2. 信息安全负责人		身份证号			
现住地址					
传呼		手机		联系电话	
是否参加过计算机信息安全员培训并取得合格证					
个人工作简历					

3. 技术负责人		身份证号			
现住地址					
传呼		手机		联系电话	
是否参加过计算机信息安全员培训并取得合格证					
个人工作简历					

网吧其他从业人员																			
姓名	身份证号																		备注
4.																			
5.																			
6.																			
7.																			
8.																			
9.																			

互联网上网服务营业场所现场安全检查表

检查单位：　　　　　　　　　　　　　　　　　　　　　　时间：　年　月　日

网吧名称		负责人		联系电话	
网吧地址				联系电话	
联网方式	□ ADSL □ ISDN □ DDN □ 微波 □ HFC □ 光纤			有（ ）个互联网接入 IP	
（固定 IP）互联网接入 IP 地址					
（固定 IP）互联网接入账号				上网电话	
场地实际经营面积			（ ）m^2		
提供上网服务的计算机数量			（ ）台		
有无专用配电箱			有（ ）无（ ）		
是否三相四线电源接入			是（ ）否（ ）		
有无漏电开关			是（ ）否（ ）		
有无应急照明措施			有（ ）无（ ）		
上网计算机是否采用单机单插方式供电			是（ ）否（ ）		
有无悬挂“禁止吸烟”标志			有（ ）无（ ）		
有无制定和公示安全管理制度			有（ ）无（ ）		
有无制定和公示上网登记制度			有（ ）无（ ）		
有无公示有关法律、法规及建立场内巡查制度			有（ ）无（ ）		
有无安装防黄、防病毒软件			有（ ）无（ ）		
有无公示 110、119 及网络安全报警电话			有（ ）无（ ）		
有无擅自停止实施安全保护技术措施			有（ ）无（ ）		
有无擅自更改地址或改建、扩建，变更计算机数量			有（ ）无（ ）		
有无按规定核对、登记上网人员的有效身份证件			有（ ）未严格落实（ ）无（ ）		
有无按规定保存、备份计算机信息系统日志记录 60 日以上			有（ ）保存不全面（ ）无（ ）		
消防安全通道是否健全、畅通			有通道（ ）个 畅通（ ）封堵（ ）		
内部网络设置情况	安全管理系统是否正常运行		正常（ ）不正常（ ）未安装（ ）		
	内部网络设置情况与上报材料是否一致		一致（ ）不一致（ ）		
	网络结构是否符合安全要求或被擅自更改		符合（ ）不符合（ ）有更改（ ）		
	采用何种实名制管理系统或管理软件				
安全员姓名		证书编号		培训日期	
安全员姓名		证书编号		培训日期	
检查结果：					

检查民警签名：　　　　　　　　　　　　　　　　联系电话：

网吧负责人签名：

网络安全检查意见书

** 公网检查[201　] 　号

根据《互联网上网服务营业场所管理条例》规定，经审核，已安装互联网上网服务营业场所安全管理软件，符合开办互联网上网服务营业场所网络安全要求。

营业场所名称：

法人代表：　　　　　　　　　　网吧负责人：

经营地址：

计算机台数：

年　月　日

互联网上网服务营业场所安全责任书

________公安局：

为加强对本营业场所的管理，促进健康文明上网，确保网络与信息安全，根据《互联网上网服务营业场所管理条例》和有关法律法规的规定，本单位特作出如下保证：

一、遵守法律、行政法规和其他有关规定，提供良好的服务，加强行业自律，接受有关部门依法实施的监督管理。

二、在营业场所的显著位置悬挂地级市以上公安部门制定的《上网安全守则》。

三、要求消费者必须凭有效身份证件(身份证、学生证、军人证、护照)上机；建立上网用户登记制度，对上网用户姓名、单位、住址、证件号码、用机代码及用机起止时间等内容进行登记，登记记录保存期不得少于60日，系统必须具备完善的日志文件管理功能，日志文件保存期不得少于60日。

四、不利用互联网上网服务营业场所制作、下载、复制、查阅、发布、传播或者以其他方式使用含有下列内容的信息：

(一) 反对《宪法》确定的基本原则的；

(二) 危害国家统一、主权和领土完整的；

(三) 泄露国家秘密、危害国家安全或者损害国家荣誉和利益的；

(四) 煽动民族仇恨、民族歧视、破坏民族团结，或者侵害民族风俗、习惯的；

(五) 破坏国家宗教政策，宣扬邪教、迷信的；

(六) 散布谣言，扰乱社会秩序，破坏社会稳定的；

(七) 宣传淫秽、赌博、暴力或者教唆犯罪的；

(八) 侮辱或者诽谤他人，侵害他人合法权益的；

(九) 危害社会公德或者民族优秀文化传统的；

(十) 含有法律、行政法规禁止的其他内容的。

五、不进行下列危害信息网络安全的活动：

(一) 故意制作或者传播计算机病毒以及其他破坏性程序的；

(二) 非法侵入计算机信息系统或者破坏计算机信息系统功能、数据和应用程序的；

(三) 进行法律、行政法规禁止的其他活动的。

六、落实技术措施防治计算机病毒和防范网络攻击，及时更新和下载系统补丁。

七、不转借、转让账号。落实网络信息安全管理措施，制止、举报违法犯罪行为。

八、对利用本场所从事的违法犯罪行为予以制止，保留操作记录，并在24小时内及时向所在地公安机关举报。

九、变更名称、住所、法定代表人或者主要负责人、注册资本、网络地址或者终止经营活动，到公安机关办理有关手续或者备案。

责任单位：(盖章)

单位法人代表(负责人)：(签字)

年　　月　　日

互联网上网服务营业场所上网安全守则

为加强对互联网上网服务营业场所的管理，促进健康文明上网，根据《互联网上网服务营业场所管理条例》和有关法律法规的规定制定本上网安全守则。

一、"网吧"等互联网上网服务营业场所和上网消费者应当遵守国家法律、法规和有关

规定，不得从事危害国家安全、泄露国家秘密，侵犯国家、社会、集体利益和公民合法权益的活动。

二、“网吧”等互联网上网服务营业场所和上网消费者不得利用互联网上网服务营业场所制作、下载、复制、查阅、发布、传播或者以其他方式使用含有下列内容的信息：

（一）反对宪法规定的基本原则的；

（二）危害国家统一、主权和领土完整的；

（三）泄露国家秘密，危害国家安全或者损害国家荣誉和利益的；

（四）煽动民族仇恨、民族歧视，破坏民族团结，或者侵害民族风俗、习惯的；

（五）破坏国家宗教政策，宣扬邪教、迷信的；

（六）散布谣言，扰乱社会秩序，破坏社会稳定的；

（七）宣传淫秽、赌博、暴力或者教唆犯罪的；

（八）侮辱或者诽谤他人，侵害他人合法权益的；

（九）危害社会公德或者民族优秀文化传统的；

（十）含有法律、行政法规禁止的其他内容的。

三、“网吧”等互联网上网服务营业场所和上网消费者不得进行下列危害信息网络安全的活动：

（一）故意制作或者传播计算机病毒以及其他破坏性程序的；

（二）非法侵入计算机信息系统或者破坏计算机信息系统功能、数据和应用程序的；

（三）进行法律、行政法规禁止的其他活动的。

四、“网吧”等互联网上网服务营业场所应当通过依法取得经营许可证的互联网接入服务提供者以局域网的方式接入互联网，不得采取其他方式接入互联网。

五、“网吧”等互联网上网服务营业场所和上网消费者不得利用网络游戏或者其他方式进行赌博或者变相赌博活动。

六、“网吧”等互联网上网服务营业场所应当建立场内巡查制度，发现上网消费者有违法行为的，应当立即予以制止并向公安机关举报。

七、“网吧”等互联网上网服务营业场所应当对上网消费者的身份等有效证件进行核对、登记，并记录有关上网信息。登记内容和记录备份保存时间不得少于 60 日，并在公安机关依法查询时予以提供。登记内容和记录备份在保存期内不得修改或者删除。

八、“网吧”等互联网上网服务营业场所应当依法履行信息网络安全职责，不得擅自停止实施安全技术措施，不得擅自增加上网机器，不得擅自改变网络结构。

公民、法人和其他组织有权对“网吧”等互联网上网服务营业场所和上网者进行社会监督，发现违法犯罪行为，应当及时向所在地公安机关报告。

报警电话：

电子邮箱：

** 市公安局公共信息网络安全保卫部门

5.3.3 基础资料管理

根据网吧开业审核内容和日常安全检查实际情况，建立本地网吧基础资料库，网吧地址、网吧法定代表人及联系电话、网吧固定 IP 地址、网吧计算机总数等关键资料应及时更新入库。

5.4 违反互联网上网服务营业场所安全管理的处罚

违反互联网上网服务营业场所安全管理规定的法律责任，主要有三种：一是刑事责任，即触犯刑法规定应承担的法律责任；二是民事责任，即违反民事法律规范应承担的法律责任；三是行政责任，即违反行政管理法律规定应承担的法律责任。《互联网上网服务营业场所管理条例》主要涉及刑事责任和行政责任。

5.4.1 刑事处罚

互联网上网服务营业场所经营单位违反条例的规定，触犯刑律的，依法追究刑事责任。可能构成的犯罪主要包括以下几种：如果行为人利用互联网上的赌博信息聚众赌博，就有可能构成赌博罪；如果行为人利用互联网传播淫秽信息，就有可能构成传播淫秽物品罪；如果行为人利用互联网传播有害信息，从事分裂祖国、破坏国家安定团结等罪恶勾当，危害国家安全，就有可能构成危害国家安全罪；如果行为人擅自设立互联网上网服务营业场所，或擅自从事互联网上网服务经营活动的，就有可能构成非法经营罪。由司法机关根据行为性质，依照刑法的有关规定来认定。

上网消费者利用互联网上网服务营业场所制作、复制、传播有害信息的，触犯刑律的，应依法追究刑事责任。

5.4.2 行政处罚

互联网上网服务营业场所经营单位违反条例的规定，尚不够刑事处罚的，可以采取以下行政处罚措施。

(1) 警告：由公安机关对行为人给予警告，告诫其及时改正，不得再犯。

(2) 没收违法所得：只要有违法所得，不论其情节轻重，一律由公安机关予以没收。

(3) 罚款：有违法经营额的，由公安机关依法给予罚款。

(4) 如果情节严重，社会危害性比较大，还可以采取责令停业整顿和吊销《网络文化经营许可证》的行政处罚。

(5) 行政拘留：限制违反国家安全或治安管理秩序的行为的短期人身自由的处罚，由公安机关执行。

上网消费者利用互联网上网服务营业场所制作、复制、传播有害信息，尚不够刑事处罚

的，由公安机关依照治安管理处罚法的规定给予处罚，若违法了其他有关法律、行政法规的，还可以依照这些法律法规进行处罚。

5.4.3　法律责任

违反《互联网上网服务营业场所管理条例》应承担的法律责任主要包括：

（1）擅自设立互联网上网服务营业场所，或者擅自从事互联网上网服务经营活动的，由工商行政管理部门或者由工商行政管理部门会同公安机关依法予以取缔，查封其从事违法经营活动的场所，扣押从事违法经营活动的专用工具、设备；触犯刑律的，依照刑法关于非法经营罪的规定，依法追究刑事责任；尚不够刑事处罚的，由工商行政管理部门没收违法所得及其从事违法经营活动的专用工具、设备；违法经营额一万元以上的，并处违法经营额 5 倍以上 10 倍以下的罚款；违法经营额不足一万元的，并处一万元以上五万元以下的罚款。

（2）互联网上网服务营业场所经营单位涂改、出租、出借或者以其他方式转让《网络文化经营许可证》，触犯刑律的，依照刑法关于伪造、变造、买卖国家机关公文、证件、印章罪的规定，依法追究刑事责任；尚不够刑事处罚的，由文化行政部门吊销《网络文化经营许可证》，没收违法所得；违法经营额五千元以上的，并处违法经营额 2 倍以上 5 倍以下的罚款；违法经营额不足五千元的，并处五千元以上一万元以下的罚款。

（3）互联网上网服务营业场所经营单位利用营业场所制作、下载、复制、查阅、发布、传播或者以其他方式使用有害信息，触犯刑律的，依法追究刑事责任；尚不够刑事处罚的，由公安机关给予警告，没收违法所得；违法经营额一万元以上的，并处违法经营额 2 倍以上 5 倍以下的罚款；违法经营额不足一万元的，并处一万元以上二万元以下的罚款；情节严重的，责令停业整顿，直至由文化行政部门吊销《网络文化经营许可证》。

上网消费者有前款违法行为，触犯刑律的，依法追究刑事责任；尚不够刑事处罚的，由公安机关依照治安管理处罚条例的规定给予处罚。

（4）互联网上网服务营业场所经营单位有下列行为之一的，由文化行政部门给予警告，可以并处一万五千元以下的罚款；情节严重的，责令停业整顿，直至吊销《网络文化经营许可证》：

① 在规定的营业时间以外营业的。

② 接纳未成年人进入营业场所的。

③ 经营非网络游戏的。

④ 擅自停止实施经营管理技术措施的。

⑤ 未悬挂《网络文化经营许可证》或者未成年人禁入标志的。

（5）互联网上网服务营业场所经营单位有下列行为之一的，由文化行政部门、公安机关依据各自职权给予警告，可以并处一万五千元以下的罚款；情节严重的，责令停业整顿，直至由文化行政部门吊销《网络文化经营许可证》：

① 向上网消费者提供的计算机未通过局域网的方式接入互联网的。

② 未建立场内巡查制度，或者发现上网消费者的违法行为未予制止并向文化行政部

门、公安机关举报的。

③ 未按规定核对、登记上网消费者的有效身份证件或者记录有关上网信息的。

④ 未按规定时间保存登记内容、记录备份，或者在保存期内修改、删除登记内容、记录备份的。

⑤ 变更名称、住所、法定代表人或者主要负责人、注册资本、网络地址或者终止经营活动，未向文化行政部门、公安机关办理有关手续或者备案的。

(6) 互联网上网服务营业场所经营单位有下列行为之一的，由公安机关给予警告，可以并处一万五千元以下的罚款；情节严重的，责令停业整顿，直至由文化行政部门吊销《网络文化经营许可证》：

① 利用明火照明或者发现吸烟不予制止，或者未悬挂禁止吸烟标志的。

② 允许带入或者存放易燃、易爆物品的。

③ 在营业场所安装固定的封闭门窗栅栏的。

④ 营业期间封堵或者锁闭门窗、安全疏散通道或者安全出口的。

⑤ 擅自停止实施安全技术措施的。

(7) 违反国家有关信息网络安全、治安管理、消防管理、工商行政管理、电信管理等规定，触犯刑律的，依法追究刑事责任；尚不够刑事处罚的，由公安机关、工商行政管理部门、电信管理机构依法给予处罚；情节严重的，由原发证机关吊销许可证件。

(8) 互联网上网服务营业场所经营单位被处以吊销《网络文化经营许可证》行政处罚的，应当依法到工商行政管理部门办理变更登记或者注销登记；逾期未办理的，由工商行政管理部门吊销营业执照。

(9) 互联网上网服务营业场所经营单位被吊销《网络文化经营许可证》的，自被吊销《网络文化经营许可证》之日起五年内，其法定代表人或者主要负责人不得担任互联网上网服务营业场所经营单位的法定代表人或者主要负责人。擅自设立的互联网上网服务营业场所经营单位被依法取缔的，自被取缔之日起五年内，其主要负责人不得担任互联网上网服务营业场所经营单位的法定代表人或者主要负责人。

习　　题

1. 互联网上网服务营业场所中禁止制作、下载、复制、查阅、发布、传播的十类有害信息是什么？

2. 互联网上网服务营业场所存在哪些安全问题？

3. 公安机关对互联网上网服务营业场所的管理职责包括哪些内容？

4. 互联网上网服务营业场所信息网络安全管理制度主要包括哪些？

5. 对互联网上网服务营业场所进行的安全审核包括哪几个方面？具体的要求有哪些？

第 6 章

信息安全等级保护管理

【内容提要】

本章介绍信息安全等级保护管理工作中所涉及的相关内容。通过学习，要求学生了解我国信息安全等级保护制度、信息安全等级保护政策与标准，重点掌握我国信息系统等级保护工作内容及各项具体工作流程。

我国已建成规模宏大、覆盖全国的信息网络，重要网络和信息系统在政府机构、企业单位及社会团体的日常事件和人们的工作生活中发挥着越来越多的重要作用。

组织开展对重要网络和信息系统的信息安全等级保护工作是公安机关在信息网络领域开展的面向全社会的管理监察工作，是公安机关在社会信息化条件的一项新职责。实施信息安全等级保护是公安机关依法保障重要信息系统安全的重要手段。《人民警察法》和《中华人民共和国计算机信息系统安全保护条例》规定了公安机关负责监督管理信息系统特别是重点领域信息系统安全保护工作。

6.1 信息安全等级保护制度

信息安全等级保护制度是保障国家信息安全，促进国家信息化建设健康发展的基本制度和基本国策，由国家强制实施，是我国信息安全保障的政策体系。信息安全等级保护是指对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。

1. 信息安全等级保护制度建设的原因

1）信息安全形势严峻

我们国家的基础网络和信息系统日益遭受着国内外不法分子的入侵、攻击、破坏。窃取国家秘密，给国家安全带来了严重威胁。

针对信息网络和信息系统的违法犯罪持续上升。网上盗窃、网络淫秽色情、网络赌博、网络入侵攻击等网络违法犯罪日益猖獗。

信息网络和信息系统安全隐患严重。我国很多单位和部门使用大量国外的信息技术产品、信息安全产品和信息服务，给我国的信息安全，特别是信息网络和信息系统的安全埋下

了安全隐患。

2）维护国家安全的需要

信息网络与信息系统已成为我国的关键基础设施，建立信息安全等级保护这一基本制度、基本策略才能更有效地保护这些重要信息。

信息安全是国家安全的重要组成部分，做好信息安全保障也就是保障好国家安全。

2. 信息安全等级保护制度的原则

信息安全等级保护的核心是对信息安全分等级、按标准进行建设、管理和监督。信息安全等级保护制度遵循以下基本原则：

（1）明确责任，共同保护。通过信息安全等级保护，组织和动员国家、法人和其他组织、公民共同参与信息安全等级保护工作；各单位各部门主体按照规范和标准分别承担相应的、明确具体的信息安全等级保护责任。

（2）依照标准，自行保护。国家运用强制性的规范及标准，要求信息网络和信息系统按照相应的建设和管理要求，自主定级、自行保护。

（3）同步建设，动态调整。信息系统在新建、改建、扩建时应当同步建设信息安全设施，保障信息安全与信息化建设相适应。因信息网络和信息系统的应用类型、范围等条件的变化及其他原因，信息安全保护等级需要变更，应当根据信息安全等级保护的管理规范和技术标准的要求，重新确定信息系统的安全保护等级。等级保护的管理规范和技术标准应按照等级保护工作开展的实际情况适时修订。

（4）指导监督，重点保护。国家指定信息安全监管职能部门通过备案、指导、检查、督促整改等方式，对重要信息和信息系统的信息安全保护工作进行指导监督。国家重点保护涉及国家安全、经济命脉、社会稳定的基础信息网络和重要信息系统，主要包括：国家事务处理信息系统（党政机关办公系统）；财政、金融、税务、海关、审计、工商、社会保障、能源、交通运输、国防工业等关系到国计民生的信息系统；教育、国家科研等单位的信息系统；公用通信、广播电视传输等基础信息网络中的信息系统；网络管理中心、重要网站中的重要信息系统和其他领域的重要信息系统。

3. 信息安全等级保护制度的主要内容

1）信息和信息系统分等级实行安全保护

根据信息和信息系统在国家安全、经济建设、社会生活中的重要程度；遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度；针对信息的保密性、完整性和可用性要求及信息系统必须达到的基本安全保护水平等因素，2007 年下发的《信息安全等级保护管理办法》中将信息和信息系统划分为以下五个安全保护和监管等级：

- 第一级为自主保护级，适用于一般的信息和信息系统，其受到破坏后，会对公民、法人和其他组织的权益有一定影响，但不危害国家安全、社会秩序、经济建设和公共利益。依照国家管理规范和技术标准进行自主保护。

- 第二级为指导保护级，适用于一定程度上涉及国家安全、社会秩序、经济建设和公共利益的一般信息和信息系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成一定损害。在信息安全监管职能部门指导下依照国家管理规范和技术标准进行自主保护。
- 第三级为监督保护级，适用于涉及国家安全、社会秩序、经济建设和公共利益的信息和信息系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成较大损害。依照国家管理规范和技术标准进行自主保护，信息安全监管职能部门对其进行监督、检查。
- 第四级为强制保护级，适用于涉及国家安全、社会秩序、经济建设和公共利益的重要信息和信息系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成严重损害。依照国家管理规范和技术标准进行自主保护，信息安全监管职能部门对其进行强制监督、检查。
- 第五级为专控保护级，适用于涉及国家安全、社会秩序、经济建设和公共利益的重要信息和信息系统的核心子系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成特别严重损害。依照国家管理规范和技术标准进行自主保护，国家指定专门部门、专门机构进行专门监督。

国家通过制定统一的管理规范和技术标准，组织行政机关、公民、法人和其他组织根据信息和信息系统的不同重要程度开展有针对性的保护工作。国家对不同安全保护级别的信息和信息系统实行不同强度的监管政策。

2）国家对信息安全产品的使用实行分等级管理

按照信息安全产品的可控性、可靠性、安全性和可监督性的要求确定相应等级进行管理。不同安全保护等级的信息系统和网络应使用与其安全等级相适应的信息安全产品。

- 可控性是指国家或用户对产品的技术可控。可控性的主要内容包括：产品具有我国自主知识产权、产品源代码可由国家或用户掌握、用户是否可控制产品的配置等。
- 可靠性是指生产信息安全产品的单位和人员稳定可靠。可靠性的主要内容包括：生产信息安全产品单位和人员的背景、规模、流动性、社会关系、经济状况、法律能力、特许授权、专业能力和有关资质认证等。
- 安全性是指不会因使用该信息安全产品而给信息系统引入安全隐患。安全性的主要内容包括：信息安全产品是否有漏洞、后门，远程控制功能用户是否可知可控等。
- 可监督性指产品的研发生产和检测过程可监督。可监督性的内容主要包括：产品的研发生产和检测过程各环节的方式、结果的真实性可验证，产品的源代码可托管等。

3）信息安全事件实行分等级响应和处置

依据信息安全事件对信息和信息系统的破坏程度、所造成的社会影响以及涉及的范围，

确定事件等级。根据不同安全保护等级的信息系统中发生的不同等级事件制定相应的预案,确定事件响应和处置的范围、程度以及适用的管理制度等。信息安全事件发生后,分等级按照预案进行响应和处置。

- 一是根据信息安全事件的不同危害程度和所发生的系统的安全级别,事先划定信息安全事件的等级。
- 二是根据不同等级的安全事件,制定相应的响应和处置预案。
- 三是一旦发生信息安全事件,根据其危害和发生的部位,迅速确定事件等级,并根据等级启动相应的响应和处置预案。

4. 信息安全等级保护制度的特点

(1) 紧迫性。紧迫性的原因就是我国信息安全滞后于信息化发展。我们国家的信息网络和信息系统在建设之初一般重应用、轻安全。

(2) 全面性。信息安全等级保护的内容涉及广泛,涉及安全架构,安全领导机构,安全组织,安全管理,安全技术,灾备、应急、监控、风险评估。其与我们国家信息安全保障工作的主要内容基本一致;同时信息安全等级保护工作要求社会各单位各部门都要落实。

(3) 基础性。信息安全等级保护制度是国家的基本制度、基本国策。需要全面实施,并且相关职能部门要对这项工作的实施进行监督检查指导。

(4) 强制性。从国家法律、国务院文件规定我们国家的信息安全等级保护工作是强制实施的,国家把这项工作任务赋予了公安机关,由公安机关来监督、检查、指导。

(5) 规范性。我们国家的信息安全等级保护工作有相应的政策引导,有相应的标准保障。

6.2 信息安全等级保护政策与标准

6.2.1 信息安全等级保护政策体系

近几年,公安部根据《中华人民共和国计算机信息系统安全保护条例》即国务院 147 号令的授权,会同国家保密局、国家密码管理局、国家发改委、原国务院信息办等出台了一系列信息安全等级保护管理规范、行业规范、部委文件,公安部还对信息安全等级保护的具体工作出台了一系列指导意见和规范,这些都构成了信息安全等级保护政策体系。

1. 信息安全等级保护总体方面的政策文件

《关于信息安全等级保护工作的实施意见》(公通字[2004]66 号)和《信息安全等级保护管理办法》(公通字[2007]43 号)两个文件确定了等级保护制度的总体内容和要求,对等级保护工作的开展起到宏观指导作用。

(1)《关于信息安全等级保护工作的实施意见》(公通字[2004]66 号)。该文件是由公安部、国家保密局、国家密码管理局、国务院信息化工作办公室共同会签印发、指导相关部

门实施信息安全等级保护工作的纲领性文件，主要内容包括贯彻落实信息安全等级保护制度的基本原则，等级保护工作的基本内容、工作要求和实施计划以及各部门工作职责分工等。

(2)《信息安全等级保护管理办法》(公通字[2007]43 号)。该文件是在开展信息系统安全等级保护基础调查工作和信息安全等级保护试点工作基础上，由公安部、国家保密局、国家密码管理局、国务院信息化工作办公室共同会签印发的重要管理规范，主要内容包括信息安全等级保护制度的基本内容、流程及工作要求，系统定级、备案、安全建设整改、等级测评的实施与管理，信息安全产品和测评机构选择等，为开展信息安全等级保护工作提供了规范保障。

2. 信息安全等级保护具体环节的政策规范

对应等级保护工作的具体环节(信息系统定级、备案、安全建设整改、等级测评、安全检查)出台了相应的政策规范，这些政策规范对于开展信息安全等级保护的任务，职责分工，主要内容有着明确的要求：

1) 定级环节

《关于开展全国重要信息系统安全等级保护定级工作的通知》(公信安[2007]861 号)，该通知部署在全国范围内开展重要信息系统安全等级保护定级工作，标志着全国信息安全等级保护工作全面开展。该文件由公安部、国家保密局、国家密码管理局、国务院信息化工作办公室共同会签印发。

2) 备案环节

《信息安全等级保护备案实施细则》(公信安[2007]1360 号)，该文件规定了公安机关受理信息系统运营使用单位信息系统备案工作的内容、流程、审核等内容，并附带有关法律文书，指导各级公安机关受理信息系统备案工作。该文件由公安部网络安全保卫局印发。

3) 安全建设整改环节

《关于开展信息系统等级保护安全建设整改工作的指导意见》(公信安[2009]1429 号)，该文件明确了非涉及国家秘密信息系统开展安全建设整改工作的目标、内容、流程和要求等，文件附件包括《信息安全等级保护安全建设整改工作指南》和《信息安全等级保护主要标准简要说明》。该文件由公安部印发。

《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》(发改高技[2008]2071 号)，该文件要求非涉密国家电子政务项目开展等级测评和信息安全风险评估要按照《信息安全等级保护管理办法》进行，明确了项目验收条件：公安机关颁发的信息系统安全等级保护备案证明、等级测评报告和风险评估报告。该文件由国家发改委、公安部、国家保密局共同会签印发。

4) 等级测评环节

《关于印发〈信息安全等级测评报告模版〉试行的通知》(公信安[2009]1487 号)，该文件明确了等级测评的内容、方法和测评报告格式等内容，用于规范等级测评活动。该文件由公

安部网络安全保卫局印发。

《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》(公信安[2010]303 号),该文件明确了等级测评的工作目标、工作内容、工作要求等,文件附件包括《信息安全等级保护测评机构申请表》、《信息安全等级保护测评机构推荐证书样式》和《信息安全等级保护测评机构检查表》。该文件由公安部网络安全保卫局印发。

5) 安全检查环节

《公安机关信息安全等级保护检查工作规范》(公信安[2008]736 号),该文件规定了公安机关开展信息安全等级保护检查工作的内容、程序、方式以及相关法律文书等,使检查工作规范化、制度化。该文件由公安部网络安全保卫局印发。

《关于开展信息安全系统等级保护专项监督检查工作的通知》(公信安[2010]1175 号),该文件明确了公安机关开展信息安全等级保护检查工作的检查目的、检查内容、检查方式、进度安排等。该文件由公安部网络安全保卫局印发。

6.2.2 信息安全等级保护标准体系

为推动我国信息安全等级保护工作的开展,十几年来在有关部门的领导和支持下,在国内有关专家、企业的共同努力下,全国信息安全标准化技术委员会和公安部信息系统安全标准化技术委员会组织制订了信息安全等级保护工作需要的一系列标准,形成了比较完整的信息安全等级保护标准体系,为开展信息安全等级保护工作提供了标准保障。信息安全等级保护标准体系如图 6-1 所示。各单位各部门信息系统安全建设整改工作应依据《信息安全等级保护基本要求》或行业标准规范,并在不同阶段、针对不同技术活动参照相应的标准规范进行。等级保护相关标准与各工作环节的关系如图 6-2 所示。

1. 信息安全等级保护标准分类

1) 基础标准

- 《计算机信息系统安全保护等级划分准则》(GB 17859—1999)。
- 《信息系统安全等级保护基本要求》(GB/T 22239—2008)。

2) 应用类标准

(1) 信息系统等级保护定级。

《信息系统安全保护等级定级指南》(GB/T 22240—2008)。

(2) 信息系统等级保护实施。

《信息系统安全等级保护实施指南》(信安字[2007]10 号)。

(3) 信息系统安全建设与管理。

- 《信息系统通用安全技术要求》(GB/T 20271—2006)。
- 《信息系统等级保护安全设计技术要求》(信安秘字[2009]059 号)。
- 《信息系统安全管理要求》(GB/T 20269—2006)。
- 《信息系统安全工程管理要求》(GB/T 20282—2006)。

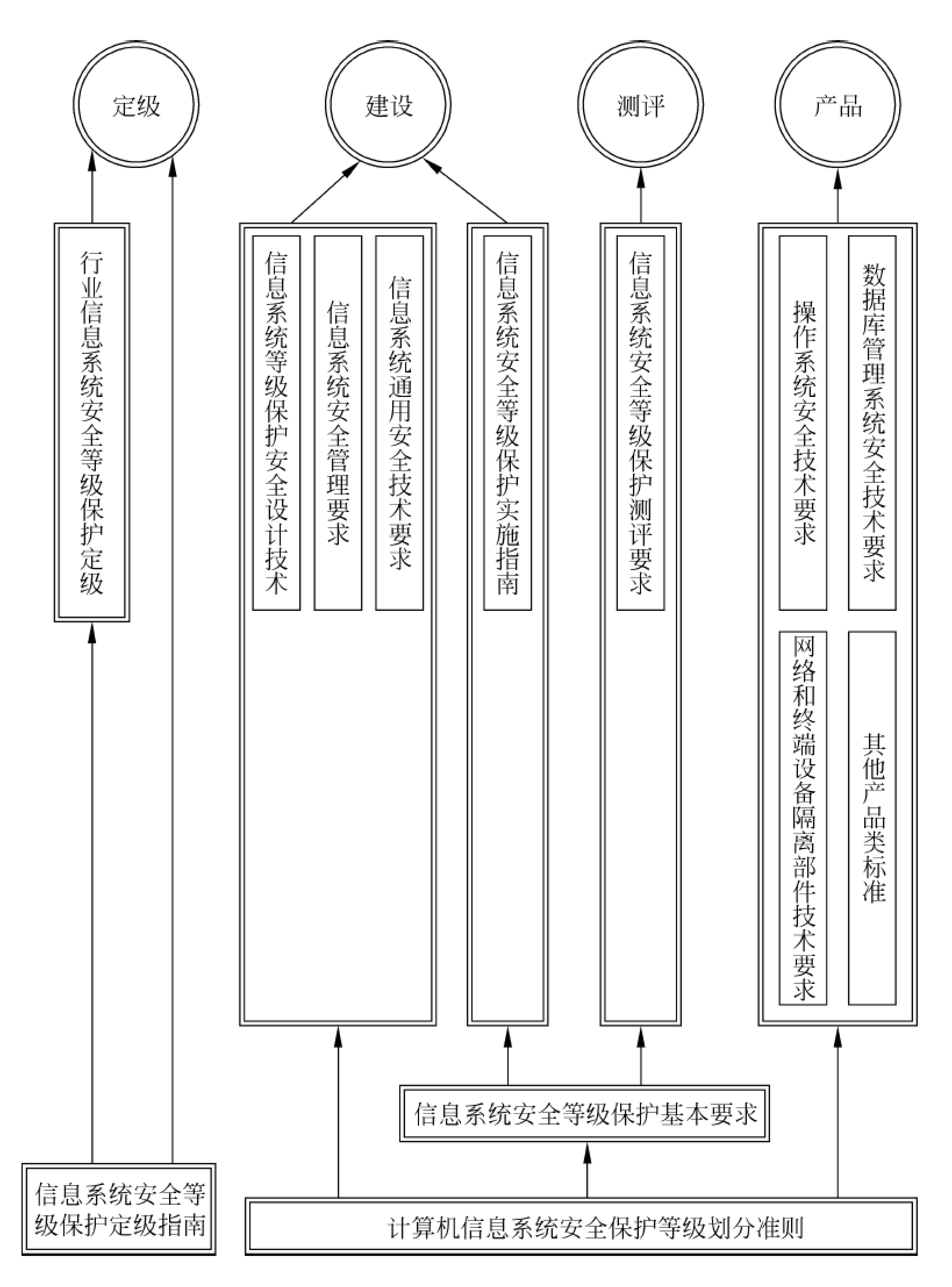


图 6-1　信息安全等级保护相关标准体系

- 《信息系统物理安全技术要求》(GB/T 21052—2007)。
- 《网络基础安全技术要求》(GB/T 20270—2006)。
- 《信息系统安全等级保护体系框架》(GA/T 708—2007)。
- 《信息系统安全等级保护基本模型》(GA/T 709—2007)。
- 《信息系统安全等级保护基本配置》(GA/T 710—2007)。

(4) 信息系统等级保护测评。

- 《信息系统安全等级保护测评要求》(报批稿)。

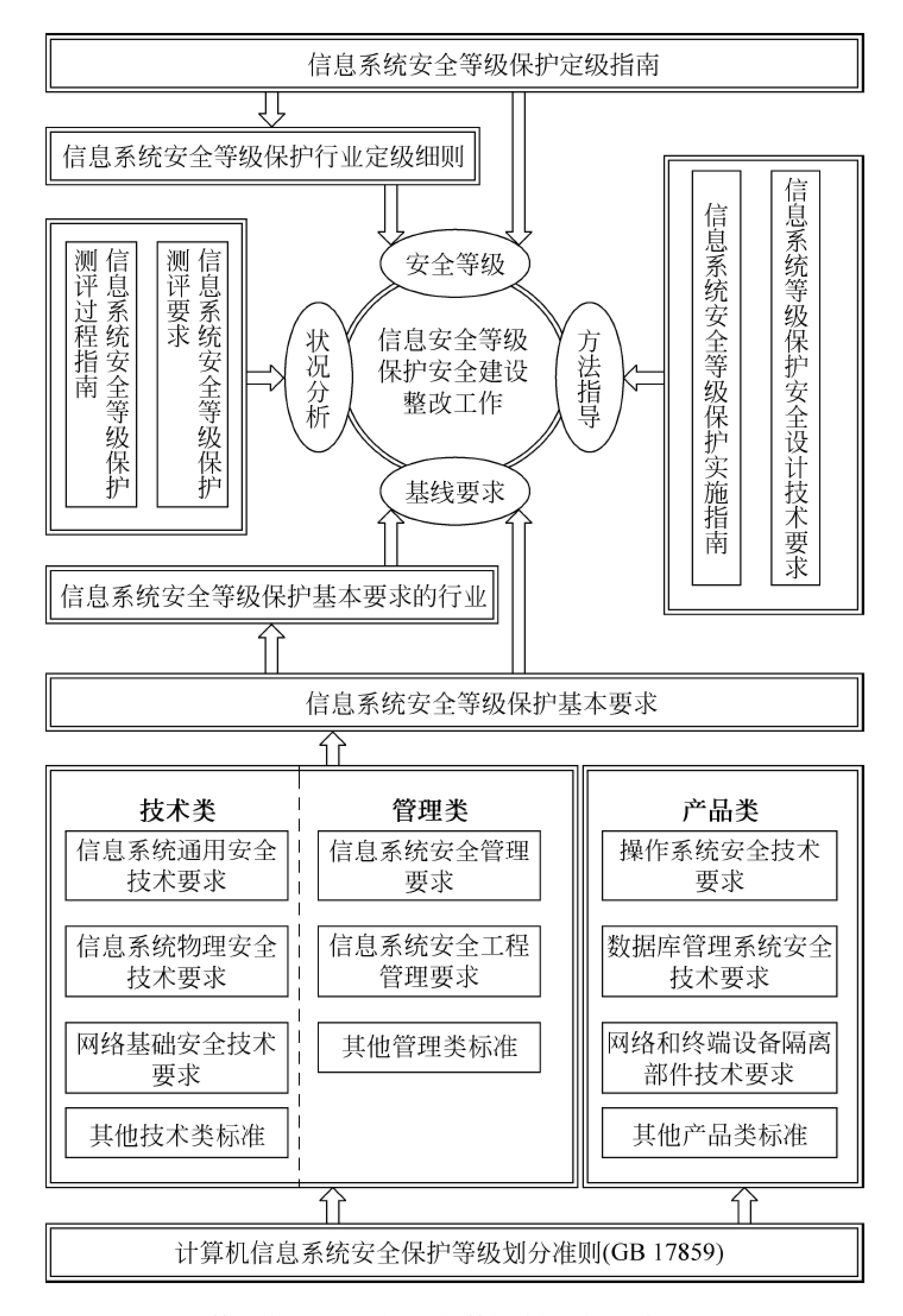


图 6-2　等级保护相关标准与等级保护各工作环节的关系

- 《信息系统安全等级保护测评过程指南》(报批稿)。
- 《信息系统安全管理测评》(GA/T 713—2007)。

3) 产品类标准

(1) 操作系统。

- 《操作系统安全技术要求》(GB/T 20272—2006)。
- 《操作系统安全评估准则》(GB/T 20008—2005)。

（2）数据库。

- 《数据库管理系统安全技术要求》(GB/T 20273—2006)。
- 《数据库管理系统安全评估准则》(GB/T 20009—2005)。

（3）网络。

- 《网络端设备隔离部件技术要求》(GB/T 20279—2006)。
- 《网络端设备隔离部件测试评价方法》(GB/T 20277—2006)。
- 《网络脆弱性扫描产品技术要求》(GB/T 20278—2006)。
- 《网络脆弱性扫描产品测试评价方法》(GB/T 20280—2006)。
- 《网络交换机安全技术要求》(GA/T 684—2007)。
- 《虚拟专用网安全技术要求》(GA/T 686—2007)。

（4）PKI。

- 《公钥基础设施安全技术要求》(GA/T 687—2007)。
- 《PKI 系统安全等级保护技术要求》(GB/T 21053—2007)。

（5）网关。

- 《网关安全技术要求》(GA/T 681—2007)。

（6）服务器。

- 《服务器安全技术要求》(GB/T 21028—2007)。

（7）入侵检测。

- 《入侵检测系统技术要求和检测方法》(GB/T 20275—2006)。
- 《计算机网络入侵分级要求》(GA/T 700—2007)。

（8）防火墙。

- 《防火墙安全技术要求》(GA/T 683—2007)。
- 《防火墙技术测评方法》(报批稿)。
- 《信息系统安全等级保护防火墙安全配置指南》(报批稿)。
- 《防火墙技术要求和测评方法》(GB/T 20281—2006)。
- 《包过滤防火墙评估准则》(GB/T 20010—2005)。

（9）路由器。

- 《路由器安全技术要求》(GB/T 18018—2007)。
- 《路由器安全评估准则》(GB/T 20011—2005)。
- 《路由器安全测评要求》(GA/T 682—2007)。

（10）交换机。

- 《网络交换机安全技术要求》(GB/T 21050—2007)。
- 《交换机安全测评要求》(GA/T 685—2007)。

（11）其他产品。

- 《终端计算机系统安全等级技术要求》(GA/T 671—2006)。

- 《终端计算机系统测评方法》(GA/T 671—2006)。
- 《审计产品技术要求和测评方法》(GB/T 20945—2006)。
- 《虹膜特征识别技术要求》(GB/T 20979—2007)。
- 《虚拟专网安全技术要求》(GA/T 686—2007)。
- 《应用软件系统安全等级保护通用技术指南》(GA/T 711—2007)。
- 《应用软件系统安全等级保护通用测试指南》(GA/T 712—2007)。
- 《网络和终端设备隔离部件测试评价方法》(GB/T 20277—2006)。
- 《网络脆弱性扫描产品测评方法》(GB/T 20280—2006)。

4) 其他类标准。

(1) 风险评估。

- 《信息安全风险评估规范》(GB/T 20984—2007)。

(2) 事件管理。

- 《信息安全事件管理指南》(GB/Z 20985—2007)。
- 《信息安全事件分类分级指南》(GB/Z 20986—2007)。
- 《信息系统灾难恢复规范》(GB/T 20988—2007)。

2. 应用有关标准需注意的问题

(1)《信息系统安全等级保护基本要求》只是阶段性目标,《信息系统通用安全技术要求》、《信息系统等级保护安全设计技术要求》等才是实现该目标的方法和途径。

(2)《信息系统安全等级保护基本要求》中不包含安全设计和工程实施等方面内容,因此应参照《信息系统通用安全技术要求》、《信息系统等级保护安全设计技术要求》等应用标准进行。所有类型的标准要综合使用。

(3) 重点行业可以按照《信息系统安全等级保护基本要求》等国家标准,结合行业特点和特殊安全需求,在公安部等有关部门指导下,制定行业标准规范或细则,指导行业信息系统等级保护的工作。

6.3 信息系统等级保护工作

6.3.1 信息系统等级保护工作的要求与职责

1. 信息安全等级保护工作的要求

信息安全等级保护工作要突出重点、分级负责、分类指导、分步实施,按照谁主管谁负责、谁运营谁负责的要求,明确主管部门以及信息系统建设、运行、维护、使用单位和个人的安全责任,分别落实等级保护措施。实施信息安全等级保护应当做好以下六个方面工作:

(1) 完善标准,分类指导。制定系统完整的信息安全等级保护管理规范和技术标准,并根据工作开展的实际情况不断补充完善。信息安全监管职能部门对不同重要程度的信息和

信息系统的安全等级保护工作给予相应的指导，确保等级保护工作顺利开展。

(2) 科学定级，严格备案。信息和信息系统的运营、使用单位按照等级保护的管理规范和技术标准，确定其信息和信息系统的安全保护等级，并报其主管部门审批同意。

对于包含多个子系统的信息系统，在保障信息系统安全互联和有效信息共享的前提下，应当根据等级保护的管理规定、技术标准和信息系统内各子系统的重要程度，分别确定安全保护等级。跨地域的大系统实行纵向保护和属地保护相结合的方式。

国务院信息化工作办公室组织国内有关信息安全专家成立信息安全保护等级专家评审委员会。重要的信息和信息系统的运营、使用单位及其主管部门在确定信息和信息系统的安全保护等级时，应请信息安全保护等级专家评审委员会给予咨询评审。

安全保护等级在三级以上的信息系统，由运营、使用单位报送本地区地市级公安机关备案。跨地域的信息系统由其主管部门向其所在地的同级公安机关进行总备案，分系统分别由当地运营、使用单位向本地地市级公安机关备案。

信息安全产品使用的分等级管理以及信息安全事件分等级响应、处置的管理办法由公安部会同保密局、国密办、工业与信息化部和认监委等部门制定。

(3) 建设整改，落实措施。对已有的信息系统，其运营、使用单位根据已经确定的信息安全保护等级，按照等级保护的管理规范和技术标准，采购和使用相应等级的信息安全产品，建设安全设施，落实安全技术措施，完成系统整改。对新建、改建、扩建的信息系统应当按照等级保护的管理规范和技术标准进行信息系统的规划设计、建设施工。

(4) 自查自纠，落实要求。信息和信息系统的运营、使用单位及其主管部门按照等级保护的管理规范和技术标准，对已经完成安全等级保护建设的信息系统进行检查评估，发现问题及时整改，加强和完善自身信息安全等级保护制度的建设，加强自我保护。

(5) 建立制度，加强管理。信息和信息系统的运营、使用单位按照与本系统安全保护等级相对应的管理规范和技术标准的要求，定期进行安全状况检测评估，及时消除安全隐患和漏洞，建立安全制度，制定不同等级信息安全事件的响应、处置预案，加强信息系统的安全管理。信息和信息系统的主管部门应当按照等级保护的管理规范和技术标准的要求做好监督管理工作，发现问题，及时督促整改。

(6) 监督检查，完善保护。公安机关按照等级保护的管理规范和技术标准的要求，重点对第三、第四级信息和信息系统的安全等级保护状况进行监督检查。发现确定的安全保护等级不符合等级保护的管理规范和技术标准的，要通知信息和信息系统的主管部门及运营、使用单位进行整改；发现存在安全隐患或未达到等级保护的管理规范和技术标准要求的，要限期整改，使信息和信息系统的安全保护措施更加完善。同时还对信息系统中使用的信息安全产品的等级进行监督检查。

对第五级信息和信息系统的监督检查，由国家指定的专门部门、专门机构按照有关规定进行。国家保密工作部门、密码管理部门以及其他职能部门按照职责分工指导、监督、检查。

2. 信息安全等级保护工作的职责

《信息安全等级保护管理办法》中第二条至第五条明确了国家、信息安全监管部门、信息系统主管部门、信息系统运营使用单位的责任义务。

第二条明确了国家的责任：国家通过制定统一的信息安全等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统分等级实行安全保护，对等级保护工作的实施进行监督、管理。

第三条明确了信息安全监管部门的职责：信息安全监管部门（包括公安机关、保密部门、国家密码工作部门）组织制定等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统实行分等级安全保护，对等级保护工作的实施进行监督、管理。公安机关负责信息安全等级保护工作的监督、检查、指导。国家保密工作部门负责等级保护工作中有关保密工作的监督、检查、指导。国家密码管理部门负责等级保护工作中有关密码工作的监督、检查、指导。涉及其他职能部门管辖范围的事项，由有关职能部门依照国家法律法规的规定进行管理。国务院信息化工作办公室及地方信息化领导小组办事机构负责等级保护工作的部门间协调。

在信息安全等级保护工作中，坚持“分工负责、密切配合”的原则。公安机关牵头，负责全面工作的监督、检查、指导，国家保密工作部门、国家密码管理部门配合，国务院信息化工作办公室及地方信息化领导小组办事机构协调；涉及国家秘密的信息系统，主要由国家保密工作部门负责，其他部门参与、配合。因为涉及国家秘密信息系统中也会发生信息安全问题和密码问题；非涉及国家秘密的信息系统，主要由公安机关负责，其他部门参与、配合。因为非涉及国家秘密信息系统中也会发生保密问题和密码问题。一方为主负责某一领域工作，其他相关部门参与、配合。需要强调的是，涉及工作秘密的信息系统不属于涉密信息系统，不能将涉密信息系统扩大化。当信息系统难以认定是否属于涉密信息系统时，可以由信息系统运营使用单位、公安机关、国家保密工作部门共同认定。

第四条明确了信息系统主管部门的责任义务：信息系统主管部门依照《信息安全等级保护管理办法》及相关标准规范，督促、检查、指导本行业、本部门或者本地区信息系统运营、使用单位的信息安全等级保护工作。

第五条明确了运营使用单位的责任义务：信息系统运营使用单位按照国家有关等级保护的管理规范和技术标准开展等级保护工作，建设安全设施、建立安全制度、落实安全责任，接受公安机关、保密部门、国家密码工作部门对信息安全等级保护工作的监督、指导，保障信息系统安全。

公民、法人和其他组织应当按照国家有关等级保护的管理规范和技术标准开展等级保护工作，服从国家对信息安全等级保护工作的监督、指导，保障信息系统安全。信息安全产品的研制、生产单位，信息系统的集成、等级测评、风险评估等安全服务机构，依据国家有关管理规定和技术标准，开展技术服务、技术支持等工作，并接受信息安全监管部门的监督管理。

6.3.2　信息系统等级保护工作流程

1. 信息系统等级保护定级工作

公安部、国家保密局、国家密码管理局、国务院信息化工作办公室联合下发《关于开展全国重要信息系统安全等级保护定级工作的通知》(公信安[2007]861 号),定于 2007 年 7 月至 10 月在全国范围内组织开展重要信息系统安全等级保护定级工作。

1) 定级范围

(1) 电信、广电行业的公用通信网、广播电视传输网等基础信息网络,经营性公众互联网信息服务单位、互联网接入服务单位、数据中心等单位的重要信息系统。

(2) 铁路、银行、海关、税务、民航、电力、证券、保险、外交、科技、发展改革、国防科技、公安、人事劳动和社会保障、财政、审计、商务、水利、国土资源、能源、交通、文化、教育、统计、工商行政管理、邮政等行业、部门的生产、调度、管理、办公等重要信息系统。

(3) 市(地)级以上党政机关的重要网站和办公信息系统。

(4) 涉及国家秘密的信息系统(以下简称涉密信息系统)。

2) 定级工作的主要内容

(1) 开展信息系统基本情况的摸底调查。各行业主管部门、运营使用单位要组织开展对所属信息系统的摸底调查,全面掌握信息系统的数量、分布、业务类型、应用或服务范围、系统结构等基本情况,按照《信息系统等级保护管理办法》和《信息系统安全等级保护定级指南》的要求,确定定级对象。各行业主管部门要根据行业特点提出指导本地区、本行业定级工作的具体意见。

(2) 初步确定安全保护等级。各信息系统主管部门和运营使用单位要按照《信息系统等级保护管理办法》和《信息系统安全等级保护定级指南》,初步确定定级对象的安全保护等级,起草定级报告。跨省或者全国统一联网运行的信息系统可以由主管部门统一确定安全保护等级。涉密信息系统的等级确定按照国家保密局的有关规定和标准执行。

(3) 评审与审批。初步确定信息系统安全保护等级后,可以聘请专家进行评审。对拟确定为第四级以上信息系统的,由运营使用单位或主管部门请国家信息安全保护等级专家评审委员会评审。运营使用单位或主管部门参照评审意见最后确定信息系统安全保护等级,形成定级报告。当专家评审意见与信息系统运营使用单位或其主管部门意见不一致时,由运营使用单位或主管部门自主决定信息系统安全保护等级。信息系统运营使用单位有上级行业主管部门的,所确定的信息系统安全保护等级应当报经上级行业主管部门审批同意。

(4) 备案。根据《信息系统等级保护管理办法》,信息系统安全保护等级为第二级以上的信息系统运营使用单位或主管部门到公安部网站下载《信息系统安全等级保护备案表》和辅助备案工具,持填写的备案表和利用辅助备案工具生成的备案电子数据,到公安机关办理备案手续,提交有关备案材料及电子数据文件。其中,第二级信息系统的备案单位只需填写

备案表中的表一、表二和表三，第三级以上信息系统的备案单位还应当同时提交备案表表四所列各项内容的书面材料。隶属于中央的在京单位，其跨省或者全国统一联网运行并由主管部门统一定级的信息系统，由主管部门向公安部办理备案手续。跨省或者全国统一联网运行的信息系统在各地运行、应用的分支系统，向当地设区的市级以上公安机关备案。

涉密信息系统建设使用单位依据《信息系统等级保护管理办法》和国家保密局的有关规定，填写《涉及国家秘密的信息系统分级保护备案表》，按照属地化管理原则，中央和国家机关单位的涉密信息系统向国家保密局备案；地方单位的涉密信息系统向所在地的市(地)级以上保密工作部门备案；中央和国家机关地方所属单位的涉密信息系统，向所在地的省级保密工作部门备案。

(5) 备案管理。公安机关和国家保密工作部门负责受理备案并进行备案管理。信息系统备案后，公安机关应当对信息系统的备案情况进行审核，对符合等级保护要求的，颁发信息系统安全保护等级备案证明。发现不符合《信息系统等级保护管理办法》及有关标准的，应当通知备案单位予以纠正。发现定级不准的，应当通知运营使用单位或其主管部门重新审核确定。各级保密工作部门加强对涉密信息系统定级工作的指导、监督和检查。

3) 定级工作的要求

(1) 加强领导，落实保障。各地区、各部门要加强对本地区、本行业信息安全等级保护工作的组织领导，及时掌握工作进展情况，并可组织成立专家组，明确技术支持力量。信息系统运营使用单位要成立等级保护工作组，落实责任部门、责任人员和经费，保障定级工作顺利进行。

(2) 明确责任，密切配合。定级工作由各级公安机关牵头，会同国家保密工作部门、国家密码管理部门和信息化领导小组办事机构共同组织实施。各信息系统主管部门组织本行业、本部门信息系统运营使用单位开展定级工作，督促其落实定级工作各项任务。各信息系统运营使用单位依据《信息系统等级保护管理办法》和本通知要求，具体实施定级工作。

(3) 动员部署，开展培训。各地区、各部门要按照统一部署广泛进行宣传动员，举办形式多样的培训班、研讨班等，层层培训。公安部会同国家保密局、国家密码管理局、国务院信息化工作办公室对国家有关部委、各省级公安、保密、密码和信息化领导小组办事机构就《信息系统等级保护管理办法》和《信息系统安全等级保护定级指南》等内容进行培训。信息系统主管部门对所管辖的信息系统运营使用单位进行培训。各地参照上述培训模式开展培训工作。

(4) 及时总结，提出建议。各地区、各部门要结合本地区、本行业开展定级工作的实际，认真总结经验和不足，提出改进和完善定级方法的意见和建议。各地区、各部门负责等级保护的领导机构要及时总结定级工作经验，形成定级工作总结报告，并及时报送公安部。涉密信息系统定级工作总结报告向国家保密局报送。

4) 定级工作步骤

定级是等级保护工作的首要环节，是开展信息系统建设、整改、测评、备案、监督检查等

后续工作的重要基础。需要特别说明的是：信息系统的安全保护等级是信息系统的客观属性，不以已采取或将采取什么安全保护措施为依据，也不以风险评估为依据，而是以信息系统的重要性和信息系统遭到破坏后对国家安全、社会稳定、人民群众合法权益的危害程度为依据，确定信息系统的安全等级。即从国家、人民群众的根本利益出发，考虑了信息系统受到损害后的最大风险。因此，各部门、各单位要高度重视定级工作，切实加强对定级工作的组织领导，科学、准确地确定信息系统等级。信息系统运营使用单位在定级时，公安机关网络安全保卫部门可以对信息系统运营使用单位在定级工作中给予指导和帮助，保障信息系统运营使用单位科学、合理地确定定级对象和准确定级。

定级工作可以参照以下几个步骤进行。

（1）摸底调查，掌握信息系统底数。

按照《关于开展全国重要信息系统安全等级保护定级工作的通知》确定的定级范围，各部委和各省（区、市）可以组织开展对所属信息系统进行摸底调查，摸清信息系统底数；掌握信息系统（包括信息网络）的业务类型、应用或服务范围、系统结构等基本情况。各部委和各省（区、市）要加强对等级保护工作的组织领导，明确责任部门，可以成立信息安全等级保护工作领导小组（以下简称领导小组），并下设等级保护工作办公室。信息系统运营使用单位成立等级保护工作组。

相关部门工作职责：等级保护工作组对本单位的信息系统开展摸底调查，并上报领导小组办公室。领导小组办公室组织信息系统运营使用单位开展摸底调查工作，汇总信息系统摸底调查情况，报领导小组。

（2）确定定级对象。

在信息系统安全等级保护定级工作（以下简称"定级工作"）中，如何科学、合理地确定定级对象是最关键、最复杂的问题。信息系统运营使用单位或主管部门按如下原则确定定级对象：一是应用系统应按照不同业务类别单独确定为定级对象，不以系统是否进行数据交换、是否独享设备为确定定级对象条件。起传输作用的基础网络要作为单独的定级对象。二是确认负责定级的单位是否对所定级系统具有安全管理责任。三是具有信息系统的基本要素。作为定级对象的信息系统应该是由相关的和配套的设备、设施按照一定的应用目标和规则组合而成的有形实体。应避免将某个单一的系统组件（如服务器、终端、网络设备等）作为定级对象。

相关部门工作职责：等级保护工作组按照确定定级对象的原则确定本部门的定级对象，并上报领导小组办公室。公安机关指导等级保护工作组确定定级对象。专家组可以在确定定级对象过程中提供咨询指导。

（3）初步确定信息系统等级。

信息系统的安全保护等级是信息系统的客观属性，不以已采取或将采取什么安全保护措施为依据，而是以信息系统的重要性和信息系统遭到破坏后对国家安全、社会稳定、人民群众合法权益的危害程度为依据，确定信息系统的安全保护等级。既要防止个别单位片面

追求绝对安全而定级过高，也要防止为了逃避监管定级偏低。信息网络的安全等级可以参照在其上运行的信息系统的等级、网络的服务范围和自身的安全需求确定适当的保护等级，不以在其上运行的信息系统的最高等级或最低等级为标准。

跨省或者全国统一联网运行的信息系统，可以由主管部门统一确定安全保护等级。由各行业统一规划、统一建设、统一安全保护策略的信息系统，应由各部委统一确定一个级别；由各部委统一规划、分级建设、运行的信息系统，应由部、省、地市分别确定系统等级，但各行业应对该类系统提出定级意见，避免出现同类系统定级出现较大偏差问题。

① 定级的一般流程。信息系统安全包括业务信息安全和系统服务安全，与之相关的受侵害客体和对客体的侵害程度可能不同，因此，信息系统定级也应由业务信息安全和系统服务安全两方面确定。从业务信息安全角度反映的信息系统安全保护等级称业务信息安全等级。从系统服务安全角度反映的信息系统安全保护等级称系统服务安全等级。

确定信息系统安全保护等级的一般流程如图 6-3 所示。

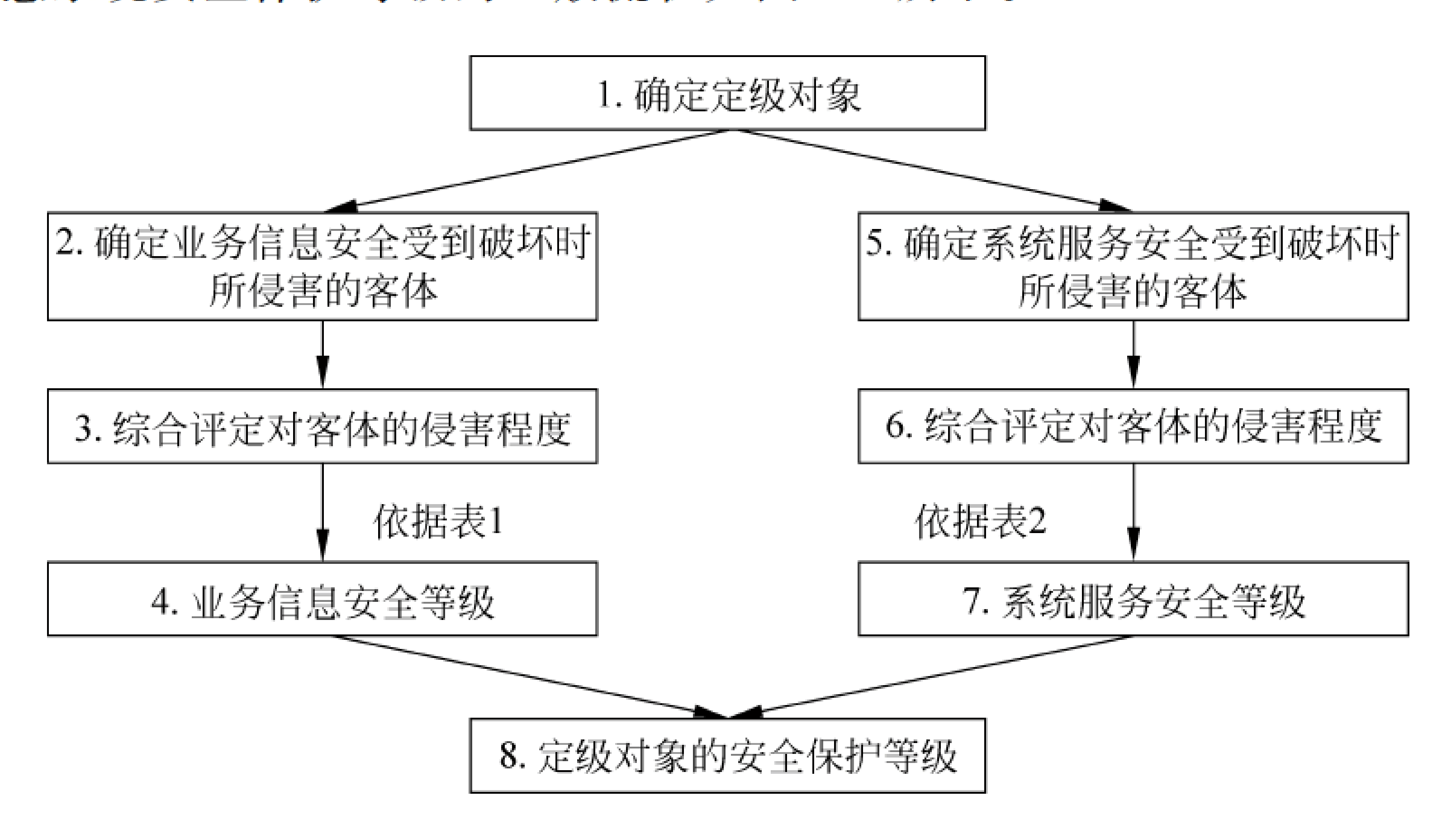


图 6-3 信息系统等级保护一般流程

② 确定受侵害的客体。定级对象受到破坏时所侵害的客体包括国家安全、社会秩序、公众利益以及公民、法人和其他组织的合法权益。

侵害国家安全的事项包括以下方面：影响国家政权稳固和国防实力；影响国家统一、民族团结和社会安定；影响国家对外活动中的政治、经济利益；影响国家重要的安全保卫工作；影响国家经济竞争力和科技实力；其他影响国家安全的事项。

侵害社会秩序的事项包括以下方面：影响国家机关社会管理和公共服务的工作秩序；影响各种类型的经济活动秩序；影响各行业的科研、生产秩序；影响公众在法律约束和道德规范下的正常生活秩序等；其他影响社会秩序的事项。

影响公共利益的事项包括以下方面：影响社会成员使用公共设施；影响社会成员获取公开信息资源；影响社会成员接受公共服务等方面；其他影响公共利益的事项。

影响公民、法人和其他组织的合法权益是指由法律确认的并受法律保护的公民、法人和其他组织所享有的一定社会权利和利益。

确定作为定级对象的信息系统受到破坏后所侵害的客体时，应首先判断是否侵害国家安全，然后判断是否侵害社会秩序或公众利益，最后判断是否侵害公民、法人和其他组织的合法权益。

各行业可根据本行业业务特点，分析各类信息和各类信息系统与国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的关系，从而确定本行业各类信息和各类信息系统受到破坏时所侵害的客体。

③ 确定对客体的侵害程度。在客观方面，对客体的侵害外在表现为对定级对象的破坏，其危害方式表现为对信息安全的破坏和对信息系统服务的破坏，其中信息安全是指确保信息系统内信息的保密性、完整性和可用性等，系统服务安全是指确保信息系统可以及时、有效地提供服务，以完成预定的业务目标。由于业务信息安全和系统服务安全受到破坏所侵害的客体和对客体的侵害程度可能会有所不同，在定级过程中，需要分别处理这两种危害方式。

信息安全和系统服务安全受到破坏后，可能产生以下危害后果：

- 影响行使工作职能。
- 导致业务能力下降。
- 引起法律纠纷。
- 导致财务损失。
- 造成社会不良影响。
- 对其他组织和个人造成损失。
- 其他影响。

④ 综合判定侵害程度。侵害程度是客观方面的不同外在表现的综合体现，因此，应首先根据不同的受侵害客体、不同危害后果分别确定其危害程度。对不同危害后果确定其危害程度所采取的方法和所考虑的角度可能不同，例如，系统服务安全被破坏导致业务能力下降的程度可以从信息系统服务覆盖的区域范围、用户人数或业务量等不同方面确定，业务信息安全被破坏导致的财物损失可以从直接的资金损失大小、间接的信息恢复费用等方面进行确定。

在针对不同的受侵害客体进行侵害程度的判断时，应参照以下不同的判别基准：

- 如果受侵害客体是公民、法人或其他组织的合法权益，则以本人或本单位的总体利益作为判断侵害程度的基准；
- 如果受侵害客体是社会秩序、公共利益或国家安全，则应以整个行业或国家的总体利益作为判断侵害程度的基准。

不同危害后果的三种危害程度描述包括：

- 一般损害。工作职能受到局部影响，业务能力有所降低但不影响主要功能的执行，

出现较轻的法律问题,较低的资产损失,有限的社会不良影响,对其他组织和个人造成较低损害。

- 严重损害。工作职能受到严重影响,业务能力显著下降且严重影响主要功能执行,出现较严重的法律问题,较高的资产损失,较大范围的社会不良影响,对其他组织和个人造成较严重损害。
- 特别严重损害。工作职能受到特别严重影响或丧失行使能力,业务能力严重下降且功能无法执行,出现极其严重的法律问题,极高的资产损失,大范围的社会不良影响,对其他组织和个人造成非常严重损害。

信息安全和系统服务安全被破坏后对客体的侵害程度,由对不同危害结果的危害程度进行综合评定得出。由于各行业信息系统所处理的信息种类和系统服务特点各不相同,信息安全和系统服务安全受到破坏后关注的危害结果、危害程度的计算方式均可能不同,各行业可根据本行业信息特点和系统服务特点,制定危害程度的综合评定方法,并给出侵害不同客体造成损害、严重损害、特别严重损害的具体定义。

⑤ 确定信息系统安全保护等级。根据业务信息安全被破坏时所侵害的客体以及对相应客体的侵害程度,依据表 6-1,即可得到业务信息安全等级。

表 6-1　业务信息安全等级矩阵表

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

根据系统服务安全被破坏时所侵害的客体以及对相应客体的侵害程度,依据表 6-2,即可得到系统服务安全等级。

表 6-2　系统服务安全等级矩阵表

系统服务安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

作为定级对象的信息系统的安全保护等级由业务信息安全等级和系统服务安全等级的较高者决定。定级对象等级确定后,可参照《信息系统安全保护等级定级报告》模板起草定级报告。

相关部门工作职责:等级保护工作组负责指导本单位相关部门确定信息系统安全保护

等级。专家组对信息系统定级提供咨询指导。主管部门对信息系统定级进行指导，也可以确定跨省或全国统一联网运行的信息系统安全保护等级。公安机关指导等级保护工作组初步确定定级对象等级。

(4) 信息系统等级评审。

在信息系统安全保护等级确定过程中，可以聘请专家进行咨询评审，并出具定级评审意见。对拟确定为第四级以上信息系统的，运营、使用单位或者主管部门应当邀请国家信息安全保护等级专家评审委员会评审，出具评审意见。评审意见及时反馈信息系统运营使用单位工作组。

相关部门工作职责：等级保护工作组可以组织专家组对信息系统安全保护等级进行评审。专家组对信息系统安全保护等级的确定进行评审，国家专家评审委员会负责第四级以上信息系统等级评审。公安机关参加定级对象安全保护等级的评审。

(5) 信息系统等级的最终确定与审批。

信息系统运营使用单位参考专家定级评审意见，最终确定信息系统等级，形成《定级报告》。如果专家评审意见与运营使用单位意见不一致时，由运营使用单位自主决定系统等级，信息系统运营使用单位有上级主管部门的，应当经上级主管部门对安全保护等级进行审核批准。主管部门一般是指行业的上级主管部门或监管部门。如果是跨地域联网运营使用的信息系统，则必须由其上级主管部门审批，确保同类系统或分支系统在各地域分别定级的一致性。

相关部门的工作职责：工作组负责组织本单位有关部门根据专家评审意见最终确定系统等级，形成《定级报告》并报领导小组办公室。领导小组办公室汇总《定级报告》，并报领导小组审批。

(6) 备案。

第二级以上信息系统，在安全保护等级确定后 30 日内，由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。运营使用单位或主管部门在备案时应填写《信息系统安全等级保护备案表》(以下简称《备案表》)提交有关备案材料及电子数据文件。定级工作的结果以备案完成为标志。相关部门的工作职责：公安机关收到备案单位提交的备案材料并材料齐全的，应向备案单位出具《信息系统安全等级保护备案材料接收回执》；备案材料不齐全的，一次性告知其补正内容。

(7) 备案审核。

受理备案的公安机关要公布备案受理地点、备案联系方式等。在受理备案时，应对提交的备案材料进行完整性审核和定级准确性审核。对符合等级保护要求的，应颁发信息系统安全等级保护备案证明。发现定级不准的，通知备案单位重新审核确定。

相关部门的工作职责：对符合等级保护要求的，公安机关将加盖本级公安机关印章的《备案表》，一份反馈备案单位，一份存档；对不符合等级保护要求的，公安机关应通知备案单位进行整改。

2. 信息系统等级保护备案工作

公安部下发的《信息安全等级保护备案实施细则》(公信安[2007]1360号)文件中规定了信息系统等级保护备案的具体内容。

1) 备案范围

非涉及国家秘密的第二级以上信息系统,应当在安全保护等级确定后30日内,由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。

新建第二级以上信息系统,应当在投入运行后30日内,由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。

隶属于中央的在京单位,其跨省或者全国统一联网运行并由主管部门统一定级的信息系统,由主管部门向公安部公共信息网络安全保卫局办理备案手续,其他信息系统由北京市公安局公共信息网络安全保卫部门受理备案。

隶属于中央的非在京单位的信息系统,由当地省级公安机关公共信息网络安全保卫部门(或其指定的地市级公安机关公共信息网络安全保卫部门)办理备案。

跨省或者全国统一联网运行的信息系统在各地运行、应用的分支系统(包括由上级主管部门定级,在当地有应用的信息系统),由所在地地市级以上公安机关公共信息网络安全保卫部门受理备案。

2) 备案工作要求

受理备案的公安机关公共信息网络安全保卫部门应该设立专门的备案窗口,配备必要的设备和警力,专门负责受理备案工作,受理备案地点、时间、联系人和联系方式等应向社会分布。

信息系统运营、使用单位或其主管部门在备案时向公安机关提交《信息系统安全等级保护备案表》(以下简称《备案表》)(一式两份)及其电子文档。第二级以上信息系统备案时需提交《备案表》中的表一、表二、表三;第三级以上信息系统还应当在系统整改、测评完成后30日内提交《备案表》表四及其有关材料。

公安机关公共信息网络安全保卫部门收到备案单位提交的备案材料后,对属于本级公安机关受理范围且备案材料齐全的,应当向备案单位出具《信息系统安全等级保护备案材料接收回执》;备案材料不齐全的,应当当场或者在五日内一次性告知其补正内容;对不属于本级公安机关受理范围的,应当书面告知备案单位到有管辖权的公安机关办理。

3) 备案审核

依据受理备案规定,公安机关网络安全保卫部门首先确认是否应当受理备案单位的备案。对属于本部门受理范围的,则需要对接收的备案材料进行审核。具体审核内容是:

一是备案符合性审查。指是否按照备案要求填写了相应的表格和文档并提供相应的电子数据文档。

二是备案表完整性审查。指备案表中表一、表二、表三所列内容是否填写完整,表四中所要求的附件内容是否齐全。

三是定级准确性审查。指提交备案的各个信息系统安全保护等级定级是否准确。

经审查，符合等级保护要求的第二级以上信息系统，应当在收到备案材料起的 10 个工作日内向备案单位颁发信息系统安全保护等级备案证明（备案证明由公安部统一监制）。不符合等级保护要求的应当在 10 个工作日内通知备案单位进行整改，同时发放《信息系统安全等级保护备案审核结果回执》及其附件，详细告知不符合标准的理由。

超过 10 个工作日仍不能审查完结的，经上级公共信息网络安全保卫部门批准，最多可以再延长 10 个工作日，并书面通知备案单位。

定级单位对公安机关审核其定级不准、提出整改意见后不服的，公安机关应建议定级单位重新组织专家进行评审，有主管部门的报其主管部门审批同意。如果专家意见与主管部门（运营使用单位）意见不一致，由主管部门（运营使用单位）自行裁定。如果裁定结果与公安机关整改要求仍不一致，可以按主管部门的意见定级，但受理备案的公共信息网络安全保卫部门必须明确其责任，告知主管部门（运营使用单位），由于定级不准而引发的一切后果由其自行承担。

受理备案的公安机关网络安全保卫部门要加强备案管理。对于拒不备案的，要向运营使用单位下发限期备案通知，逾期不备案的，要给予书面警告，并向其上级主管部门发情况通报，建议其对有关责任单位和责任人进行处理。

3. 信息系统等级保护安全建设整改工作

公安部下发的《关于开展信息系统等级保护安全建设整改工作的指导意见》（公信安[2009]1429 号）文件中规定了信息系统等级保护安全建设整改的具体内容。

1）安全建设整改范围

安全建设整改的单位主要包括三种：

（1）对已备案的第二级（含）以上信息系统纳入信息系统等级保护安全建设整改的范围。

（2）尚未定级备案的信息系统，要先定级备案、定级不准的要先纠正，再开展安全建设整改。各单位各部门不知道自己单位应该定几级的，就由公安机关或专家进行指导。同行横向其他系统或上级单位的系统定级可以作为各单位、各部门定级的参考。信息系统等级保护安全建设整改是在原来信息系统安全保护情况的基础之上，再进行安全建设整改。

（3）新建信息系统要同步开展等级保护安全建设整改工作。

依据信息系统等级保护有关政策和标准，通过组织开展信息系统等级保护安全管理制度建设、技术措施建设和等级测评，落实等级保护制度的各项要求，使信息系统安全管理水平明显提高，安全防范能力明显增强，安全隐患和安全事故明显减少，有效保障信息化健康发展，维护国家安全、社会秩序和公共利益。

2）安全建设整改工作内容

信息系统运营使用单位在开展信息系统等级保护安全建设整改工作中，应按照国家有关规定和标准规范的要求，坚持管理和技术并重的原则，将技术措施和管理措施有机结合，建

立信息系统综合防护体系，提高信息系统整体安全保护能力。具体内容如下：

（1）开展信息系统等级保护安全管理制度建设，提高信息系统安全管理水平。按照《信息安全等级保护管理办法》、《信息系统安全等级保护基本要求》、《信息系统安全管理要求》、《信息系统安全工程管理要求》等标准规范的要求，建立健全并落实符合相应等级要求的安全管理制度，建立并落实监督检查机制，定期对各项制度的落实情况进行自查和监督检查。

（2）开展信息系统等级保护安全技术措施建设，提高信息系统安全保护能力。按照《信息安全等级保护管理办法》、《信息系统安全等级保护基本要求》、《信息系统安全等级保护实施指南》、《信息系统通用安全技术要求》、《信息系统安全工程管理要求》、《信息系统等级保护安全设计技术要求》等标准规范的要求，结合行业特点和安全需求，制定符合相应等级要求的信息系统安全技术建设整改方案，开展信息系统等级保护安全技术措施建设，落实相应的物理安全、网络安全、主机安全、应用安全和数据安全等安全保护技术措施，建立并完善信息系统综合防护体系，提高信息系统的安全防护能力和水平。

（3）开展信息系统安全等级测评，使信息系统安全保护状况逐步达到等级保护要求。选择由省级（含）以上信息安全等级保护工作协调小组办公室审核并备案的测评机构，对第三级（含）以上信息系统开展等级测评工作。等级测评机构依据《信息系统安全等级保护测评要求》等标准对信息系统进行测评，对照相应等级安全保护要求进行差距分析，排查系统安全漏洞和隐患并分析其风险，提出改进建议，按照公安部制订的信息系统安全等级测评报告格式编制等级测评报告。经测评未达到安全保护要求的，要根据测评报告中的改进建议，制定整改方案并进一步进行整改。各部门要及时向受理备案的公安机关提交等级测评报告。对于重要部门的第二级信息系统，可以参照上述要求开展等级测评工作。

信息系统等级保护安全建设整改的主要工作要做到四个落实：一是落实信息安全责任制；二是落实人员安全管理制度；三是落实系统建设管理制度；四是落实系统运维管理制度。

3）安全建设整改工作流程

信息系统等级保护安全建设整改工作分为五步：

（1）制定信息系统等级保护安全建设整改工作规划，对信息系统等级保护安全建设整改工作进行总体部署。

（2）开展信息系统安全保护现状分析，从管理和技术两个方面确定信息系统等级保护安全建设整改需求。

（3）确定安全保护策略，制定信息系统等级保护安全建设整改方案。

（4）开展信息系统等级保护安全建设整改工作，建立并落实安全管理制度，落实安全责任制，建设安全设施，落实安全措施。

（5）开展安全自查和等级测评，及时发现信息系统中存在的安全隐患和威胁，进一步开展安全建设整改工作。

信息系统等级保护安全建设整改工作流程如图 6-4 所示。

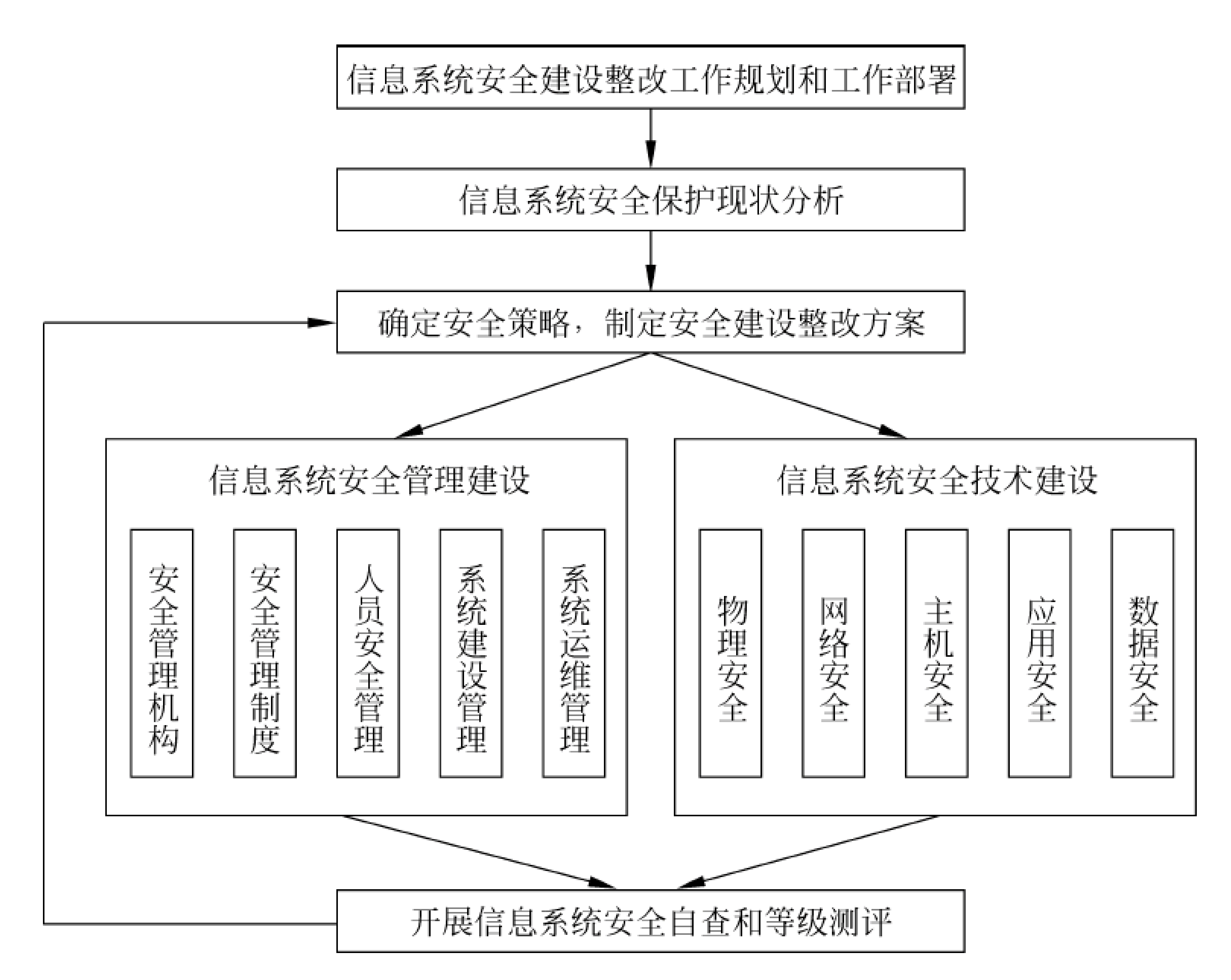


图 6-4　信息系统等级保护安全建设整改工作基本流程

4）安全建设整改工作要求

信息系统安全等级保护安全建设整改工作要求包括：

(1）统一组织，加强领导。要按照“谁主管、谁负责”的原则，切实加强对信息系统等级保护安全建设整改工作的组织领导，完善工作机制。要结合各自实际，统一规划和部署安全建设整改工作，制定安全建设整改工作实施方案。要落实责任部门、责任人员和安全建设整改经费。要利用多种形式，组织开展宣传、培训工作。

(2）循序渐进，分步实施。信息系统主管部门可以结合本行业、本部门信息系统数量、等级、规模等实际情况，按照自上而下或先重点后一般的顺序开展工作。重点行业、部门可以根据需要和实际情况，选择有代表性的第二、三、四级信息系统先进行安全建设整改和等级测评工作试点、示范，在总结经验的基础上再全面推开。

(3）结合实际，制定规范。重点行业信息系统主管部门可以按照《信息系统安全等级保护基本要求》等国家标准，结合行业特点确定具体指标；在不低于等级保护基本要求的情况下，结合系统安全保护的特殊需求，在有关部门指导下制定行业标准规范或细则，指导本行业信息系统安全建设整改工作。

(4）认真总结，按时报送。自 2009 年起，要对定级备案、等级测评、安全建设整改和自查等工作的开展情况进行年度总结，每年年底前上报同级公安机关网络安全保卫部门，各省（自治区、直辖市）公安机关网络安全保卫部门上报公安部网络安全保卫局。信息系统备案单位每半年要填写《信息安全等级保护安全建设整改工作情况统计表》并报受理备案的公安机关。

4. 信息系统等级保护等级测评工作

公安部下发的《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》(公信安[2010]303 号)文件中规定了信息系统等级保护等级测评的具体内容。

1) 测评工作目标

(1) 通过广泛宣传和正确引导,鼓励更多的有关企事业单位从事信息系统等级保护测评工作,满足信息系统等级保护测评工作的迫切需要。

(2) 通过对测评机构进行统一的能力评估和严格审核,保证测评机构的水平和能力达到有关标准规范的要求。

(3) 加强对测评机构的安全监督,规范其测评活动,保证为备案单位提供客观、公正和安全的测评服务。

(4) 督促备案单位开展等级测评工作,为开展等级保护安全建设整改工作奠定基础,使信息系统安全保护状况逐步达到等级保护要求。

2) 测评工作内容

各地要按照《关于开展信息安全等级保护安全建设整改工作的指导意见》要求,结合本地实际组织开展以下工作:

(1) 统筹规划,正确引导,积极稳妥地推动等级测评机构建设。结合本地已定级备案信息系统数量和分布情况,从满足等级测评工作的实际需要出发,统筹规划、合理布局测评机构的规模和数量,积极引导本地符合规定条件、有良好信誉的企事业单位从事等级测评工作,按照成熟一个发展一个的原则,有计划、积极稳妥地推动测评机构建设。

(2) 规范流程,严格把关,确保测评机构的水平和能力符合测评工作要求。依据《信息安全等级保护测评工作管理规范(试行)》,对申请成为测评机构的单位严格把关,按照申请受理、测评能力评估、审核、推荐的流程,认真开展测评机构评审和推荐工作。同时,要加强对等级测评机构的监督管理和指导,确保测评机构的水平和能力符合要求以及测评活动客观、公正和安全。

(3) 督促备案单位开展信息系统等级测评工作,确保安全建设整改工作的顺利开展。督促信息系统备案单位尽快委托测评机构开展等级测评,2010 年底前完成测评体系建设,并完成 30%第三级(含)以上信息系统的测评工作,2011 年底前完成第三级(含)以上信息系统的测评工作,2012 年底之前完成第三级(含)以上信息系统的安全建设整改工作。

3) 测评工作要求

(1) 高度重视,落实责任。要充分认识开展等级测评体系建设和等级测评工作的重要性,加强组织领导,落实责任。确定主管领导,落实专门管理人员,负责受理申请、审核、监督管理以及其他日常对测评机构、测评人员的管理工作。

(2) 制定计划,加强监督。要尽快确定本地等级测评体系建设和测评工作的计划,制定贯彻实施意见和方案。要督促、检查本地测评机构依据有关标准开展等级测评活动,按照《信息系统安全等级测评报告模板(试行)》(公信安[2009]1487 号)编制测评报告。

(3) 加强指导,积极宣传。要加强对本地备案单位和测评机构等级测评工作的指导,指导测评机构对测评人员开展教育培训,不断提高测评人员的安全意识和业务能力。要充分利用会议、网站和其他媒体,加大对等级测评工作有关政策和相关标准的宣传力度,推动等级测评工作的顺利开展。

4) 信息系统测评工作的主要任务和流程

等级保护测评工作的主要任务和流程如图 6-5 所示。

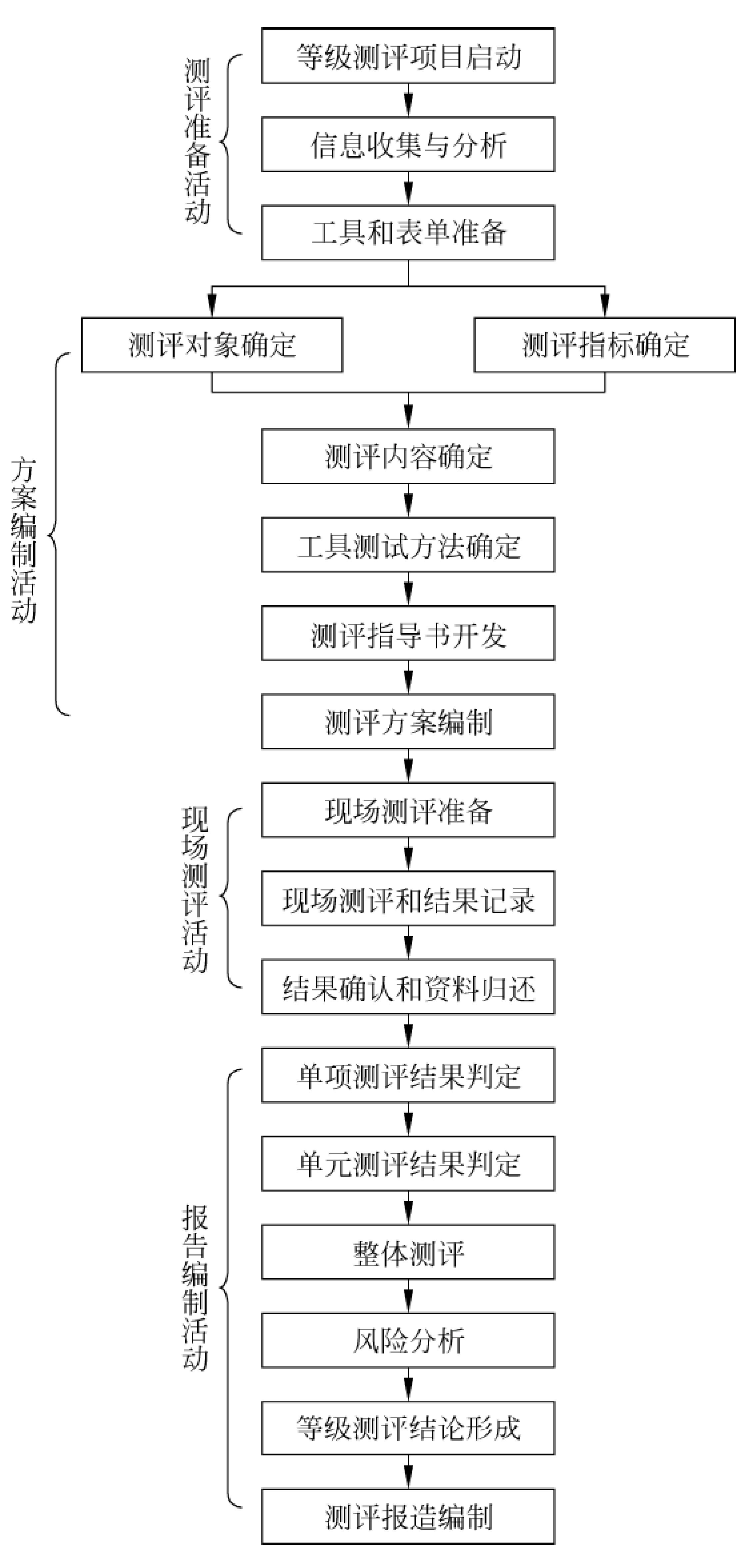


图 6-5　等级保护工作的主要内容和流程

（1）测评准备活动的主要任务包括：项目启动、信息收集和分析、工具和表单准备。这三项任务之间存在工作的先后次序，项目启动任务完成之后才能开始后续任务。可采用如图 6-6 所示的工作流程。

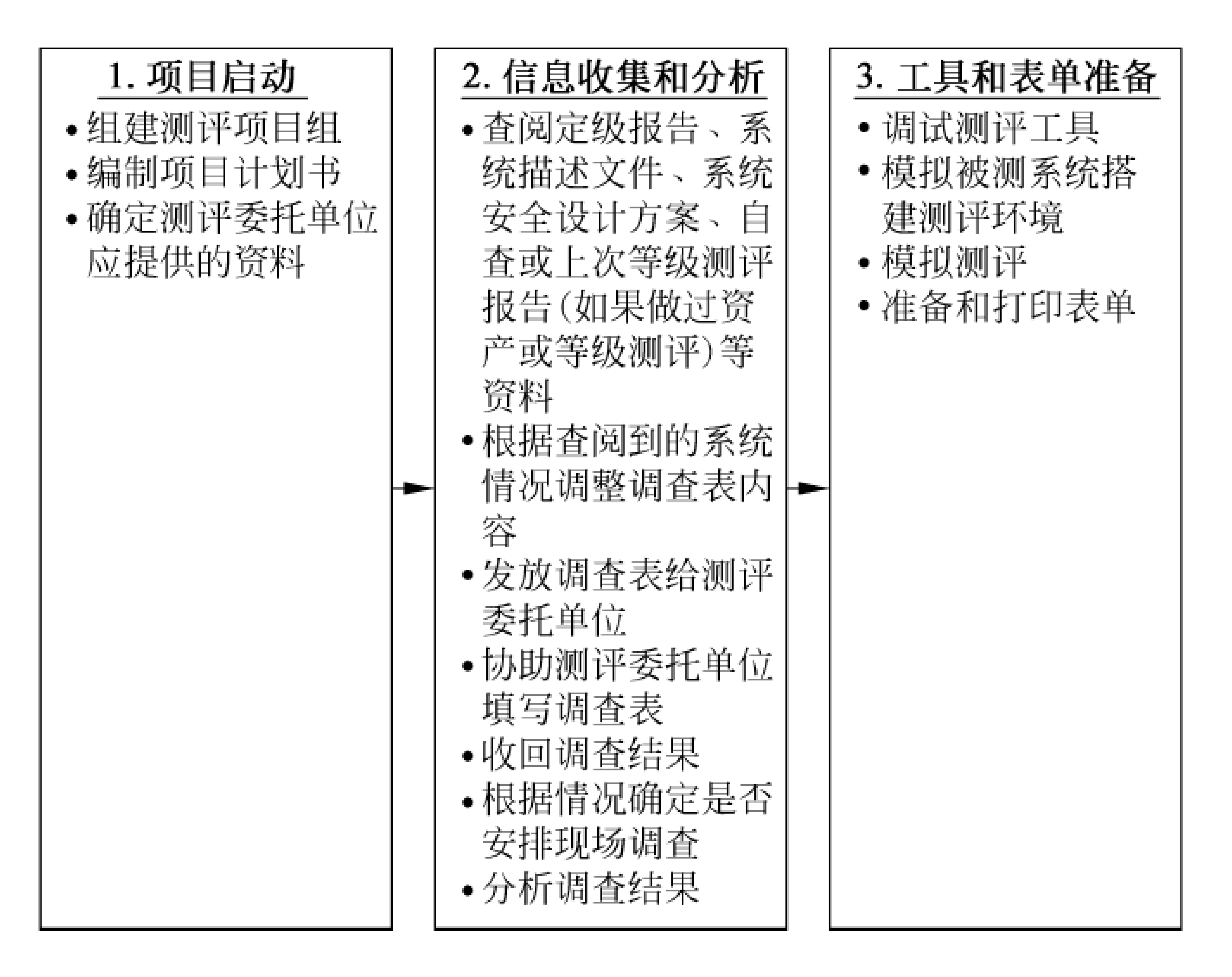


图 6-6　测评准备活动的主要任务

（2）方案编制活动的主要任务包括：测评对象确定、测评指标确定、测评内容确定、工具测试方法确定、测评指导书开发及测评方案编制六项任务。其中，测评对象确定与测评指标确定两项任务可以并行实施，其他四项任务之间存在工作的先后次序，测评内容确定任务完成之后才能开始后续任务。这六项任务可采用如图 6-7 所示的工作流程。

（3）现场测评活动的主要任务包括：现场测评准备、现场测评和结果记录、结果确认和资料归还。这三项任务之间存在工作的先后次序，现场测评准备任务完成之后才能开始后续任务。可采用如图 6-8 所示的工作流程。

（4）报告编制活动的主要任务包括：单项测评结果判定、单元测评结果判定、整体测评、风险分析、等级测评结论形成及测评报告编制。这六项任务之间存在工作的先后次序，单项测评结果判定任务完成之后才能开始后续任务。

5. 信息系统等级保护检查工作

公安部下发的《公安机关信息安全等级保护检查工作规范》（公信安[2008]736 号）文件中规定了信息系统等级保护检查的具体内容。

1）信息系统等级保护检查工作范围与原则

公安机关信息系统等级保护检查工作是指公安机关依据有关规定，会同主管部门对非涉密重要信息系统运营使用单位等级保护工作开展和落实情况进行检查，督促、检查其建设安全设施、落实安全措施、建立并落实安全管理制度、落实安全责任、落实责任部门和人员的

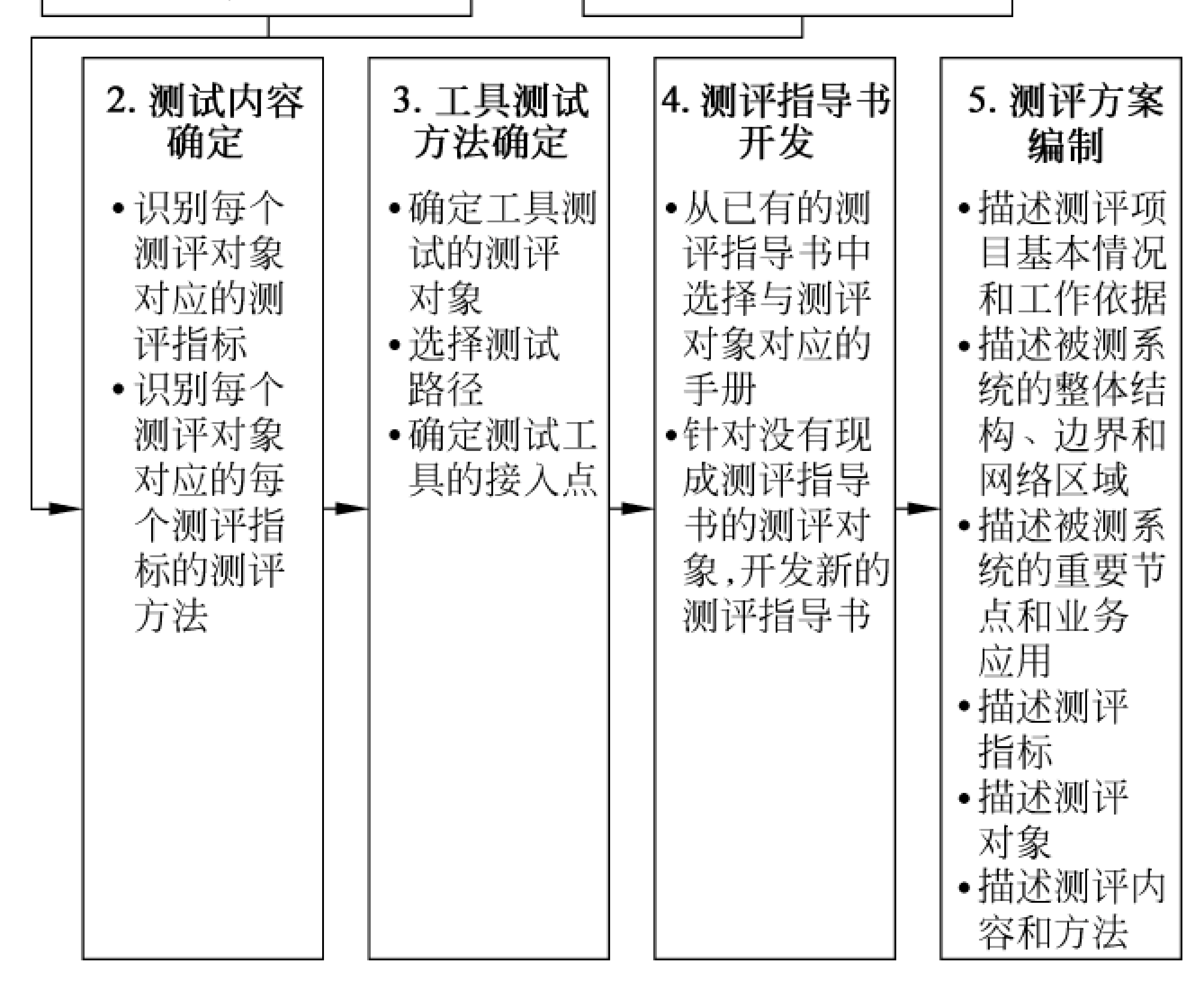


图 6-7　方案编制活动的主要任务

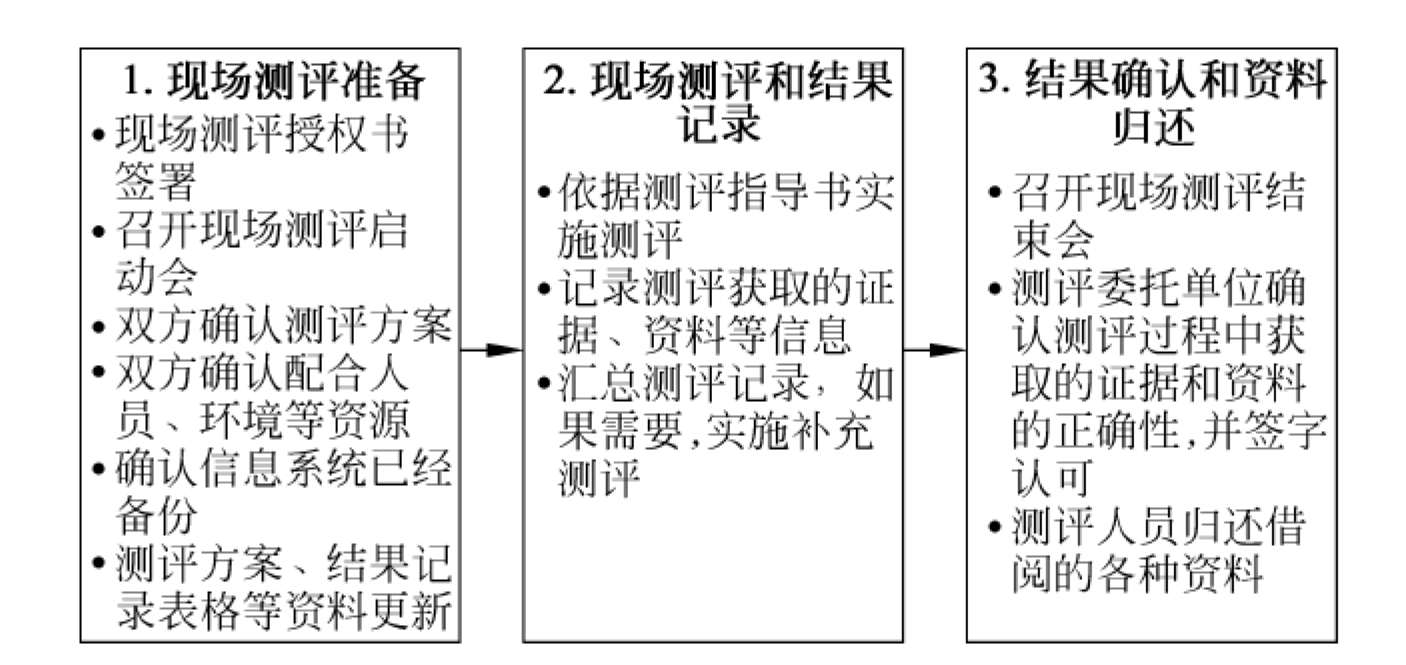


图 6-8　现场测评活动的主要任务

情况。

公安机关开展检查工作，应当按照“严格依法，热情服务”的原则，遵守检查纪律，规范检查程序，主动、热情地为运营使用单位提供服务和指导。

2）信息系统等级保护检查工作的主要内容

（1）等级保护工作组织开展、实施情况。

（2）安全责任落实情况，信息系统安全岗位和安全管理人员设置情况。

（3）按照信息安全法律法规、标准规范的要求制定具体实施方案和落实情况。

（4）信息系统定级备案情况，信息系统变化及定级备案变动情况。

（5）信息安全设施建设情况和信息安全整改情况。

（6）信息安全管理制度建设和落实情况。

（7）信息安全保护技术措施建设和落实情况。

（8）选择使用信息安全产品情况。

（9）聘请测评机构按规范要求开展技术测评工作情况，根据测评结果开展整改情况。

（10）自行定期开展自查情况及开展信息安全知识和技能培训情况。

3）信息系统等级保护检查工作的检查方式

受理备案的公安机关应当对第三级、第四级信息系统的运营使用单位的信息安全等级保护工作情况进行检查。对第三级信息系统每年至少检查一次，对第四级信息系统每半年至少检查一次。对跨省或者全国统一联网运行的信息系统的检查，应当会同其主管部门进行。对第五级信息系统，应当由国家指定的专门部门进行检查。

公安机关检查发现信息系统安全保护状况不符合信息系统等级保护有关管理规范和技术标准的，应当向运营使用单位发出整改通知。运营使用单位应当根据整改通知要求，按照管理规范和技术标准进行整改。整改完成后，应当将整改报告向公安机关备案。必要时，公安机关可以对整改情况组织检查。

习　题

1. 信息系统等级保护制度在信息系统等级保护工作中的地位和作用是什么？
2. 公安机关在信息系统等级保护工作中的职责是什么？
3. 信息系统安全等级如何划分？
4. 信息系统等级保护测评工作分为哪几个工作过程？

第 7 章

信息网络安全违法犯罪案件查处

【内容提要】

本章主要介绍网络安全保卫部门相关人员在案件查处过程中需要的基本技能和知识。通过本章的学习，掌握案件管辖范围及主要信息网络违法、犯罪案件的类型及处罚。

7.1 案件查处工作概述

7.1.1 信息网络案件的概念

信息网络案件是指行为主体违反信息网络安全管理的相关法律、法规，以计算机及信息网络为攻击、侵害对象，或以计算机及信息网络为违法犯罪工具，实施的扰乱信息网络管理秩序，危害计算机及信息网络安全，侵犯公民、法人、其他组织的合法权益或国家利益，达到立案标准，依法应当追究法律责任的案件。

7.1.2 信息网络案件管理依据

根据《公安机关内部刑事案件管辖分工》规定，网络安全保卫部门管辖的案件有：

(1) 非法侵入计算机信息系统案。

(2) 非法获取计算机信息系统数据、非法控制计算机信息系统案。

(3) 提供侵入、非法控制计算机信息系统程序、工具案。

(4) 破坏计算机信息系统案。

7.1.3 信息网络案件管辖范围

1. 主侦案件

根据公安部《关于计算机犯罪案件管辖分工问题的通知》(公通字[2000]63 号)的相关规定，《刑法》规定的非法侵入计算机信息系统案(第 285 条)和破坏计算机信息系统案(第 286 条)交由公安部公共信息网络安全保卫部门管辖。

在有条件的省级以下公安机关，上述案件交由公共信息网络安全保卫部门管辖，刑事侦查部门应予以配合和支持；公共信息网络安全保卫部门暂不具备接受上述案件条件的，仍

由刑事侦查部门管辖，公共信息网络安全保卫部门应积极协助、配合。

2. 配侦案件

（1）对于《刑法》第285条和第286条规定以外的其他涉网违法犯罪案件，由案件主办所在地的网络安全保卫部门协助办理。

（2）网络安全保卫部门应积极协助配合所在地公安机关的国保、经侦、刑侦、反邪教等警种侦办涉网违法犯罪案件。

（3）各地网络安全保卫部门应相互协作、积极配合开展协查、协捕和协助取证工作。

7.1.4 信息网络案件分类

通常将信息网络案件分为信息网络违法案件和信息网络犯罪案件两大类，二者之间的主要区别体现在如下两个方面。

1. 对社会危害不同

违法是指情节比较轻微，对社会危害性不大，没有触犯刑法，只是违反了刑法以外的法律法规的情形；而犯罪具有严重的社会危害性，触犯了刑法，应当受到刑罚处罚。

2. 处罚的方法不同

对于违法行为的处罚，民事违法行为承担民事责任，行政违法行为要受行政制裁；而犯罪则由人民法院依法判处刑罚。

违法和犯罪都是危害社会秩序、侵犯他人合法权益，应当受到法律惩处的行为，所以它们之间并没有不可逾越的鸿沟。有一般违法行为的人，如果不加以改正，发展下去就可能导致犯罪。

7.2 主要信息网络犯罪案件及其处罚标准

7.2.1 以计算机信息网络系统为对象的案件

1. 非法侵入计算机信息系统罪

《刑法》第二百八十五条规定："违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。"

【案例 1】

2010 年 5 月，某市公安机关接到当地某县交警大队报案称：2010 年 4 月至 5 月期间，该县公安局交通违章处理平台上的交通违章信息，多次遭到违法修改和删除，对该县交通违章处理信息平台造成严重破坏，致使该网站无法正常工作。

经初查发现，该县交通违章处理平台共遭到 5 次删改，删改信息达 40 余条，造成违章罚款流失近七千元，并且不法分子于 5 月 27 日对违章信息进行篡改的同时，也对该平台的工作密码进行了修改，导致工作人员无法进入系统，严重影响了该县交警大队的正常办公秩序。经工作发现，协警人员葛某有重大作案嫌疑。

葛某到案后，如实供述了其犯罪事实：2010 年 4 月的某一天，葛某经交警大队长授权进入违章处理信息平台进行正常事务性操作，同时，他因私心作祟，擅自将其亲属的车辆违章记录进行删除。一次作案得逞后，葛犯用其掌握的交警大队民警的用户名，于 4 月至 5 月，多次运用密码破译软件破解对应的登录密码，登录到公安内网交警平台进行违章数据篡改。一个月内删除系统中车辆交通违法数据 17 条，修改车辆交通违法数据 14 条，修改该系统用户密码，导致工作人员无法登录，严重干扰了该县公安局交警大队正常的道路交通管理工作，造成经济损失人民币近七千元。

法院经审理认为，葛某在未得到合法授权和批准的情况下，非法侵入某县公安局道路交通违法业务处理信息系统，并对车辆违法数据进行修改、删除和修改该系统用户密码，侵犯了该系统的安全，其行为已构成非法侵入计算机信息系统罪。根据《中华人民共和国刑法》第二百八十五条的规定，判处有期徒刑六个月。

2. 破坏计算机信息系统罪

《刑法》第二百八十六条规定，“违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。

故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。”

【案例 2】

2007 年 7 月至 9 月，一名专业的软件程序员浦某在参与编制公司软件的过程中，故意在其中安插了一个“逻辑炸弹”，在它的作用下，安装软件的计算机将会在 2007 年 10 月 1 日零时后，自动删除 C 盘至 H 盘内的所有文件。为了使软件在运行时可以执行该恶意代码，浦某还在主执行程序里添加了调用该函数的代码。当年 9 月，浦某从公司辞职，与此同时，公司也开始向市场推广了相关软件。不料，全国多家单位和个人在使用上述软件后，均出现了计算机数据被恶意删除的情况。为恢复客户计算机中被删除的数据，公司花费了 20 余万元，但仍有部分客户的计算机数据无法恢复。

法院经审理认为,浦某的行为构成破坏计算机信息系统罪,判处有期徒刑二年六个月。

7.2.2 以计算机信息网络系统为工具的案件

《刑法》第二百八十七条规定,“利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的,依照本法有关规定定罪处罚。”

1. 利用计算机信息网络危害国家安全

1) 分裂国家罪、煽动分裂国家罪

《刑法》第一百零三条规定:“组织、策划、实施分裂国家、破坏国家统一的,对首要分子或者罪行重大的,处无期徒刑或者十年以上有期徒刑;对积极参加的,处三年以上十年以下有期徒刑;对其他参加的,处三年以下有期徒刑、拘役、管制或者剥夺政治权利。

煽动分裂国家、破坏国家统一的,处五年以下有期徒刑、拘役、管制或者剥夺政治权利;首要分子或者罪行重大的,处五年以上有期徒刑。”

2) 颠覆国家政权罪、煽动颠覆国家政权罪

《刑法》第一百零五条规定:“组织、策划、实施颠覆国家政权、推翻社会主义制度的,对首要分子或者罪行重大的,处无期徒刑或者十年以上有期徒刑;对积极参加的,处三年以上十年以下有期徒刑;对其他参加的,处三年以下有期徒刑、拘役、管制或者剥夺政治权利。以造谣、诽谤或者其他方式煽动颠覆国家政权、推翻社会主义制度的,处五年以下有期徒刑、拘役、管制或者剥夺政治权利;首要分子或者罪行重大的,处五年以上有期徒刑。”

3) 间谍罪

《刑法》第一百一十条规定:“有下列间谍行为之一,危害国家安全的,处十年以上有期徒刑或者无期徒刑;情节较轻的,处三年以上十年以下有期徒刑:

(1) 参加间谍组织或者接受间谍组织及其代理人的任务的;

(2) 为敌人指示轰击目标的。”

4) 为境外窃取、刺探、收买、非法提供国家秘密情报罪

《刑法》第一百一十一条规定,“为境外的机构、组织、人员窃取、刺探、收买、非法提供国家秘密或者情报的,处五年以上十年以下有期徒刑;情节特别严重的,处十年以上有期徒刑或者无期徒刑;情节较轻的,处五年以下有期徒刑、拘役、管制或者剥夺政治权利。”

2. 利用计算机信息网络系统危害公共安全

1) 破坏电力设备罪,破坏广播电视设施、公用电信设施罪

《刑法》第一百一十八条规定:“破坏电力、燃气或者其他易燃易爆设备,危害公共安全,尚未造成严重后果的,处三年以上十年以下有期徒刑。”

《刑法》第一百一十九条规定:“破坏交通工具、交通设施、电力设备、燃气设备、易燃易爆设备,造成严重后果的,处十年以上有期徒刑、无期徒刑或者死刑。

过失犯前款罪的,处三年以上七年以下有期徒刑;情节较轻的,处三年以下有期徒刑或者拘役。”

《刑法》第一百二十四条规定："破坏广播电视设施、公用电信设施,危害公共安全的,处三年以上七年以下有期徒刑;造成严重后果的,处七年以上有期徒刑。

过失犯前款罪的,处三年以上七年以下有期徒刑;情节较轻的,处三年以下有期徒刑或者拘役。"

(编者注:此类别是指利用或侵入使用中的电力设备、广播电视设施、公用电信设施的计算机控制盒管理系统,实施破坏行为,危害公共安全的行为。)

2) 非法买卖枪支弹药罪

《刑法》第一百二十五条规定:"非法制造、买卖、运输、邮寄、储存枪支、弹药、爆炸物的,处三年以上十年以下有期徒刑;情节严重的,处十年以上有期徒刑、无期徒刑或者死刑。

非法买卖、运输核材料的,依照前款的规定处罚。

单位犯前两款罪的,对单位判处罚金,并对其直接负责的主管人员和其他直接责任人员,依照第一款的规定处罚。"

【案例3】

曾在芬兰赫尔辛基大学留学的刘某,回沪后一直待业在家,期间结识了在本市一家公司工作的周某,不久结为夫妇。周某平时十分爱好研究枪模,2005年,两人从网上购买了一支仿真手枪后,便萌生了自己也开个网站买卖枪支的想法。2006年5月,这对年轻夫妇在互联网上开设了"乐福枪模"网站,网站上张贴有各种枪支、弹药图片介绍性能和价格,并对外销售。按照夫妇俩交代,这些枪支、弹药从广州等地进货,并以网站为媒介,采用手机、电子邮件联系及QQ聊天等方式,与买家谈妥价格后,用快递送货,随后通过银行账户转账汇款成交。在一年多时间里,两人通过该网站向他人出售各类非军用枪支6把以及随枪附送的铅弹,还销售枪套等配件,价格从几十元到千元不等,获利丰厚。2006年底,徐先生在"乐福枪模"网站看中一把"北极熊"枪,于是与网站上所留的手机号码联系,周某在电话中向徐先生介绍了该枪支性能,在谈妥价格后,周某提出第一次交易用汇款方式不安全,要当面交易。于是,双方在南方商城附近接头交易,徐先生付款后,拿到了一张超市寄物箱的密码条,从寄物箱内取到了枪支。2007年初,王先生、成先生也分别在"乐福枪模"网站看中枪支,通过网站上留的手机号码取得联系,经对方介绍并谈妥价格后,分别将钱款汇至周某账户,周某用快递送货完成交易。

2007年6月,公安机关在实施全面监控,经过深入调查后,将夫妻两人抓获归案,从他们的住所内当场查获尚未售出的3支具有杀伤力的枪支,以及铅弹60余万发。

法院经审理认为,被告人周某、刘某违反法律规定,私自购买以压缩气体为动力的非军用枪支9支、气枪铅弹60余万发,其中已出售以压缩气体为动力的非军用枪支6支、气枪铅弹若干,其行为均已构成非法买卖枪支、弹药罪,且情节严重。上海市一中院以非法买卖枪支弹药罪,判处周某有期徒刑十二年,剥夺政治权利三年;妻子刘某获刑十一年,剥夺政治权利三年。

3. 利用计算机信息网络系统破坏市场经济秩序

1）侵犯著作权罪

《刑法》第二百一十七条规定："以营利为目的，有下列侵犯著作权情形之一，违法所得数额较大或者有其他严重情节的，处三年以下有期徒刑或者拘役，并处或者单处罚金；违法所得数额巨大或者有其他特别严重情节的，处三年以上七年以下有期徒刑，并处罚金：

（1）未经著作权人许可，复制发行其文字作品、音乐、电影、电视、录像作品、计算机软件及其他作品的；

（2）出版他人享有专有出版权的图书的；

（3）未经录音录像制作者许可，复制发行其制作的录音录像的；

（4）制作、出售假冒他人署名的美术作品的。"

【案例4】

盛趣信息技术（上海）有限公司拥有网络游戏《传奇世界》的著作权，2003年10月28日授权上海盛大网络发展有限公司在中国大陆地区独家运营。在《传奇世界》官服实施收费的情况下，更多的传奇玩家选择了私服，因为私服不仅仅是客观性免费游戏，而且在私服游戏中，装备的获取、等级的提升，也要比官服容易得多。这就导致国内大量《传奇世界》玩家涌入私服。2005年10月以来，盛趣信息技术（上海）有限公司从互联网上发现，浙江丽水一个网名叫"王阳"的人，使用盗版的《传奇世界》服务器端程序M5版本，架设名为"永恒大陆传奇世界"的游戏私服，引起了他们的注意。"王阳"在丽水电信、广东茂名电信等多个机房租用10余台服务器，并注册了www.sf778.com域名作为私服网站，并有专门的技术维护人员和客服人员进行营运，且非法获利数额较大，严重侵犯了该公司自主开发拥有自主知识产权的大型网络游戏《传奇世界》软件的著作权。

经工作发现，犯罪嫌疑人谢某、叶某受到利益驱使，在未经授权的情况下，从他人处非法取得能接入上海盛大网络发展有限公司《传奇世界》的程序软件，并私自架设"永恒大陆传奇世界"、"明月传世"、"沧海传世"等涉嫌侵权的网游私服，在互联网上为游戏玩家提供游戏，通过出售会员资格、游戏装备，为玩家调整级别等方式，在短短数月获取非法所得共计人民币20余万元。

本案所提到的侵犯大型网络游戏的著作权罪在《刑法》中虽有所涉及，但具体针对网络游戏侵权犯罪方面的司法解释、判例在全国非常罕见，民事侵权与刑事侵权的界线难以划分，特别是该案所涉及的司法侵权鉴定，目前国内还没有建立起一个相对规范、统一、完善的鉴定机制，加之网络犯罪中取证的要求也很高，这给实际办案带来相当大的难度。2007年5月15日，此案在当地人民法院开庭审理，法院一审判决被告人叶某构成侵犯著作权罪，判处有期徒刑三年，缓刑四年，并处罚金八万元；判处谢某构成侵犯著作权罪，判处有期徒刑三年，缓刑四年，并处罚金12.74万元。违法所得全部予以没收。

2）侵犯商业秘密罪

《刑法》第二百一十九条规定："有下列侵犯商业秘密行为之一，给商业秘密的权利人造

成重大损失的，处三年以下有期徒刑或者拘役，并处或者单处罚金；造成特别严重后果的，处三年以上七年以下有期徒刑，并处罚金：

(1) 以盗窃、利诱、胁迫或者其他不正当手段获取权利人的商业秘密的；

(2) 披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密的；

(3) 违反约定或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密的。明知或者应知前款所列行为，获取、使用或者披露他人的商业秘密的，以侵犯商业秘密论。

本条所称商业秘密，是指不为公众所知悉，能为权利人带来经济利益，具有实用性并经权利人采取保密措施的技术信息和经营信息。

本条所称权利人，是指商业秘密的所有人和经商业秘密所有人许可的商业秘密使用人。”

【案例 5】

被告人项某、孙某均是新加坡商人投资的某信息技术(上海)有限公司的软件工程师。2000 年 4 月，项某被公司派往马来西亚 ARL 公司进行门户网站建设。期间，ARL 公司曾以高薪邀项某加盟，但因故未果。因两家公司合作关系破裂，项某被本公司招回。项某因其个人要求未得到满足，对公司不满，遂积极拉拢孙某一起离开公司，加盟 ARL 公司。两人商定，孙某将其编制的软件源代码交给项某，由项某转交 ARL 公司并作演示，借此向对方推荐孙某。

同年 11 月初，项某前往马来西亚的 ARL 公司，通过新浪网的个人信箱下载了孙某从国内发出的软件源代码，并将源代码安装到 ARL 公司服务器上进行演示。此事被某信息技术(上海)有限公司发觉后，向警方报案，遂案发。一审法院经审理后认为，被告人项某、孙某违反公司有关保守商业秘密约定和要求，披露所掌握的软件源代码的商业秘密，给商业秘密权利人造成特别严重的后果，其行为已构成侵犯商业秘密罪，遂依法分别判处项某、孙某有期徒刑三年六个月和有期徒刑二年六个月，并处罚金。

3) 非法经营罪

《刑法》第二百二十五条规定：“违反国家规定，有下列非法经营行为之一，扰乱市场秩序，情节严重的，处五年以下有期徒刑或者拘役，并处或者单处违法所得一倍以上五倍以下罚金；情节特别严重的，处五年以上有期徒刑，并处违法所得一倍以上五倍以下罚金或者没收财产：

(1) 未经许可经营法律、行政法规规定的专营、专卖物品或者其他限制买卖的物品的；

(2) 买卖进出口许可证、进出口原产地证明以及其他法律、行政法规规定的经营许可证或者批准文件的；

(3) 其他严重扰乱市场秩序的非法经营行为。”

【案例 6】

2008 年 5 月 12 日，个体经营者韩某利用网上“易购币”(E-GOLD)投资返利传销活动，

致20人损失三十五万余元。当地法院以非法经营罪，判处其有期徒刑二年，缓刑三年，并处罚金二万元。

法院审理查明，2006年10月，韩某被李某（另案处理）发展为直接下线，从2006年10月初至11月底租用一地下室进行网上“易购币”投资返利传销活动。韩某用一台计算机为投资者在“WIG”网上申请一个个人邮箱，再开通一个“易购币”账户，随后便可每天得到投资额1.2%～2%不等的“易购币”利息，韩某将利息兑换成人民币返还给投资者。直接介绍别人加入者，可按投资额的10%～15%抽取介绍费；间接介绍别人加入者，上线可抽取投资额1%～2%的介绍费。此网络经营于2006年11月26日关闭，返利活动停止。期间共发展下线20人，投资五十七万余元，返利十三万余元，韩某非法获利二万余元，致投资者巨大经济损失。法院认为，韩某明知“易购币”投资返利属传销，系违法行为，但仍在利益驱使下发展下线，进行传销活动，且经营数额较大，其行为构成非法经营罪。

4. 利用计算机信息网络实施侵犯人身权利

《刑法》第二百五十三条规定：“邮政工作人员私自开拆或者隐匿、毁弃邮件、电报的，处二年以下有期徒刑或者拘役。

犯前款罪而窃取财物的，依照本法第二百六十四条的规定定罪从重处罚。

国家机关或者金融、电信、交通、教育、医疗等单位的工作人员，违反国家规定，将本单位在履行职责或者提供服务过程中获得的公民个人信息，出售或者非法提供给他人，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金。

窃取或者以其他方法非法获取上述信息，情节严重的，依照前款的规定处罚。

单位犯前两款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。”

【案例7】

2010年2月，30岁的周某注册了某信息技术有限公司，雇用了亲戚李某、张某等人，通过网上买卖企业信息、市民个人信息，大肆在网上公开“叫卖”他人的身份证号、手机号、账号、住址等“私密”信息，内容涉及房产、汽车、金融、娱乐、IT等行业，年龄涉及男女老幼，甚至连刚出生的婴儿也没能幸免，市民的个人信息被随意掌握和交易高达3000余万条。周某在事后向有关机关交代，自2005年至案发时止，她个人获利高达一百万元。而她自己开始也没感到会触犯法律。

8月5日，对涉嫌获取市民个人信息罪的李某等10名被告人进行开庭审理。法庭作出了一审，10名被告人均犯非法获取公民个人信息罪，其中9名被分别判处有期徒刑二年至拘役六个月，缓刑六个月不等，罚金四万元至一万元不等，另有1名被告人被免予刑事处罚。

5. 利用计算机信息网络实施侵犯财产

1）盗窃罪

《刑法》第二百六十四条规定：“盗窃公私财物，数额较大的，或者多次盗窃、入户盗窃、携带凶器盗窃、扒窃的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；数额巨大

或者有其他严重情节的，处三年以上十年以下有期徒刑，并处罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处罚金或者没收财产。”

《刑法》第二百六十五条规定：“以牟利为目的，盗接他人通信线路、复制他人电信码号或者明知是盗接、复制的电信设备、设施而使用的，依照本法第二百六十四条的规定定罪处罚。”

【案例 8】

2009 年 6 月 10 日，马鞍山市佳达工业园某科技公司的业务员小林像往常一样打开 QQ 邮箱，查看客户邮件。随手打开一封老客户发来的关于“供货清单”的邮件，却是个空白邮件，他当时以为是客户疏忽了，并没放在心上。令小林没有想到的是，公司第二天连续接到客户投诉，说公司网站销售平台售出的游戏点卡、手机充值卡等电子数据产品的账户、密码无法正常登录使用。技术人员将公司服务器的数据库一查，更是目瞪口呆：居然有四百多万元的电子产品不翼而飞。公司数据库中一些还未售出的电子数据产品，也被人大量地充值，或在网上低价倒卖。

警方侦查发现，源头正是小林打开的那一份空白邮件，它其实是披着“供货清单”伪装的木马程序，邮件被打开的一刹那，木马病毒就自动植入计算机系统。而幕后黑手就可以通过木马远程控制，操纵该公司计算机，盗取数据信息。警方后来通过被盗点卡充值特点，将范围锁定在了海南省海口市。专案组侦查人员随即前往海南，在一宾馆将犯罪嫌疑人抓获。

根据《刑法》第二百八十七条、第二百六十四条的规定，犯罪嫌疑人构成盗窃罪。

2）诈骗类罪

《刑法》第二百六十六条规定：“诈骗公私财物，数额较大的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；数额巨大或者有其他严重情节的，处三年以上十年以下有期徒刑，并处罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处罚金或者没收财产。本法另有规定的，依照规定。”

（1）集资诈骗罪。

《刑法》第一百九十二条规定：“以非法占有为目的，使用诈骗方法非法集资，数额较大的，处五年以下有期徒刑或者拘役，并处二万元以上二十万元以下罚金；数额巨大或者有其他严重情节的，处五年以上十年以下有期徒刑，并处五万元以上五十万元以下罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处五万元以上五十万元以下罚金或者没收财产。”

（2）贷款诈骗罪。

《刑法》第一百九十三条规定：“有下列情形之一，以非法占有为目的，诈骗银行或者其他金融机构的贷款，数额较大的，处五年以下有期徒刑或者拘役，并处二万元以上二十万元以下罚金；数额巨大或者有其他严重情节的，处五年以上十年以下有期徒刑，并处五万元以上五十万元以下罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处五万元以上五十万元以下罚金或者没收财产：

① 编造引进资金、项目等虚假理由的；

② 使用虚假的经济合同的；

③ 使用虚假的证明文件的；

④ 使用虚假的产权证明作担保或者超出抵押物价值重复担保的；

⑤ 以其他方法诈骗贷款的。”

(3) 票据诈骗罪、金融凭证诈骗罪。

《刑法》第一百九十四条规定：“有下列情形之一，进行金融票据诈骗活动，数额较大的，处五年以下有期徒刑或者拘役，并处二万元以上二十万元以下罚金；数额巨大或者有其他严重情节的，处五年以上十年以下有期徒刑，并处五万元以上五十万元以下罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处五万元以上五十万元以下罚金或者没收财产：

① 明知是伪造、变造的汇票、本票、支票而使用的；

② 明知是作废的汇票、本票、支票而使用的；

③ 冒用他人的汇票、本票、支票的；

④ 签发空头支票或者与其预留印鉴不符的支票，骗取财物的；

⑤ 汇票、本票的出票人签发无资金保证的汇票、本票或者在出票时作虚假记载，骗取财物的。

使用伪造、变造的委托收款凭证、汇款凭证、银行存单等其他银行结算凭证的，依照前款的规定处罚。”

(4) 信用证诈骗罪。

《刑法》第一百九十五条规定：“有下列情形之一，进行信用证诈骗活动的，处五年以下有期徒刑或者拘役，并处二万元以上二十万元以下罚金；数额巨大或者有其他严重情节的，处五年以上十年以下有期徒刑，并处五万元以上五十万元以下罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处五万元以上五十万元以下罚金或者没收财产：

① 使用伪造、变造的信用证或者附随的单据、文件的；

② 使用作废的信用证的；

③ 骗取信用证的；

④ 以其他方法进行信用证诈骗活动的。”

(5) 信用卡诈骗罪。

《刑法》第一百九十六条规定：“有下列情形之一，进行信用卡诈骗活动，数额较大的，处五年以下有期徒刑或者拘役，并处二万元以上二十万元以下罚金；数额巨大或者有其他严重情节的，处五年以上十年以下有期徒刑，并处五万元以上五十万元以下罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处五万元以上五十万元以下罚金或者没收财产：

① 使用伪造的信用卡，或者使用以虚假的身份证明骗领的信用卡的；

② 使用作废的信用卡的；

③ 冒用他人信用卡的；

④ 恶意透支的。

前款所称恶意透支，是指持卡人以非法占有为目的，超过规定限额或者规定期限透支，并且经发卡银行催收后仍不归还的行为。

盗窃信用卡并使用的，依照本法第二百六十四条的规定定罪处罚。”

（6）有价证券诈骗罪。

《刑法》第一百九十七条规定：“使用伪造、变造的国库券或者国家发行的其他有价证券，进行诈骗活动，数额较大的，处五年以下有期徒刑或者拘役，并处二万元以上二十万元以下罚金；数额巨大或者有其他严重情节的，处五年以上十年以下有期徒刑，并处五万元以上五十万元以下罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处五万元以上五十万元以下罚金或者没收财产。”

（7）保险诈骗罪。

《刑法》第一百九十八条规定：“有下列情形之一，进行保险诈骗活动，数额较大的，处五年以下有期徒刑或者拘役，并处一万元以上十万元以下罚金；数额巨大或者有其他严重情节的，处五年以上十年以下有期徒刑，并处二万元以上二十万元以下罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑，并处二万元以上二十万元以下罚金或者没收财产：

① 投保人故意虚构保险标的，骗取保险金的；

② 投保人、被保险人或者受益人对发生的保险事故编造虚假的原因或者夸大损失的程度，骗取保险金的；

③ 投保人、被保险人或者受益人编造未曾发生的保险事故，骗取保险金的；

④ 投保人、被保险人故意造成财产损失的保险事故，骗取保险金的；

⑤ 投保人、受益人故意造成被保险人死亡、伤残或者疾病，骗取保险金的。

有前款④、⑤所列行为，同时构成其他犯罪的，依照数罪并罚的规定处罚。

单位犯第一款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，处五年以下有期徒刑或者拘役；数额巨大或者有其他严重情节的，处五年以上十年以下有期徒刑；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑。

保险事故的鉴定人、证明人、财产评估人故意提供虚假的证明文件，为他人诈骗提供条件的，以保险诈骗的共犯论处。”

（8）合同诈骗罪。

《刑法》第二百二十四条规定：“有下列情形之一，以非法占有为目的，在签订、履行合同过程中，骗取对方当事人财物，数额较大的，处三年以下有期徒刑或者拘役，并处或者单处罚金；数额巨大或者有其他严重情节的，处三年以上十年以下有期徒刑，并处罚金；数额特别

巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处罚金或者没收财产：

① 以虚构的单位或者冒用他人名义签订合同的；

② 以伪造、变造、作废的票据或者其他虚假的产权证明作担保的；

③ 没有实际履行能力，以先履行小额合同或者部分履行合同的方法，诱骗对方当事人继续签订和履行合同的；

④ 收受对方当事人给付的货物、货款、预付款或者担保财产后逃匿的；

⑤ 以其他方法骗取对方当事人财物的。”

3）职务侵占罪

《刑法》第二百七十一条规定：“公司、企业或者其他单位的人员，利用职务上的便利，将本单位财物非法占为己有，数额较大的，处五年以下有期徒刑或者拘役；数额巨大的，处五年以上有期徒刑，可以并处没收财产。

国有公司、企业或者其他国有单位中从事公务的人员和国有公司、企业或者其他国有单位委派到非国有公司、企业以及其他单位从事公务的人员有前款行为的，依照本法第三百八十二条、第三百八十三条的规定定罪处罚。”

4）挪用资金罪

《刑法》第二百七十二条规定：“公司、企业或者其他单位的工作人员，利用职务上的便利，挪用本单位资金归个人使用或者借贷给他人，数额较大、超过三个月未还的，或者虽未超过三个月，但数额较大、进行营利活动的，或者进行非法活动的，处三年以下有期徒刑或者拘役；挪用本单位资金数额巨大的，或者数额较大不退还的，处三年以上十年以下有期徒刑。

国有公司、企业或者其他国有单位中从事公务的人员和国有公司、企业或者其他国有单位委派到非国有公司、企业以及其他单位从事公务的人员有前款行为的，依照本法第三百八十四条的规定定罪处罚。”

5）破坏生产经营罪

《刑法》第二百七十六条规定：“由于泄愤报复或者其他个人目的，毁坏机器设备、残害耕畜或者以其他方法破坏生产经营的，处三年以下有期徒刑、拘役或者管制；情节严重的，处三年以上七年以下有期徒刑。

以转移财产、逃匿等方法逃避支付劳动者的劳动报酬或者有能力支付而不支付劳动者的劳动报酬，数额较大，经政府有关部门责令支付仍不支付的，处三年以下有期徒刑或者拘役，并处或者单处罚金；造成严重后果的，处三年以上七年以下有期徒刑，并处罚金。

单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照前款的规定处罚。

有前两款行为，尚未造成严重后果，在提起公诉前支付劳动者的劳动报酬，并依法承担相应赔偿责任的，可以减轻或者免除处罚。”

6. 利用计算机信息网络破坏社会管理秩序

1）传授犯罪方法罪

《刑法》第二百九十五条规定："传授犯罪方法的，处五年以下有期徒刑、拘役或者管制；情节严重的，处五年以上十年以下有期徒刑；情节特别严重的，处十年以上有期徒刑或者无期徒刑。"

【案例 9】

2007 年 9 月下旬，江西省公安部门摧毁了号称"中国最大网游木马基地"的黑客吧。根据公安部公共信息网络安全监察局的证实，这也是目前国内首例使用网络手段犯罪后，以涉嫌传授犯罪方法罪被刑拘的案件。

2007 年 8 月 27 日，九江市公安局公共信息网络安全监察支队民警在日常网络巡查中对租用九江一家网络公司的虚拟主机，名为"黑客吧"的网站引起了好奇，该网站在首页上公开宣传是全国最大的网游木马基地。让"网上警察"更意外的是该网站收罗了"QQ 空间密码木马"、"传奇世界木马"、"劲舞团木马"、"魔兽世界木马"等各类网游木马 500 余种，而让炒股者头痛、网上淘宝网友心惊胆战、危害巨大的"网银木马"也赫然其中。江西网警调查发现，网上绰号"木马教父"的犯罪嫌疑人林某是一名在校大学生，他和他的朋友创建了"黑客吧"网站，将其服务器架设在某网络公司的机房里，该网站通过收取 VIP 会员费，向缴费网民秘密销售网游木马，提供文字、图示及动画演示的黑客教程及各种网游、网银木马下载和使用方法。

2007 年 9 月 13 日下午 5 时许，在杭州市警方配合下，公安人员来到嫌犯作案的出租屋内，只见一年轻小伙子正在"黑客吧"网站招揽客户。经审讯，该男子自称为孔某，现为浙江某大学的学生，孔某交代，这个网站是他的同学林某建立的，他只是被林某请来招揽客户，而他从每个客户中得到 30 元的提成。据孔某交代，林某正在一家美容院做面膜。民警随后在美容院抓获了林某。据林某透露，他聘请了孔某及姚某为他做客服工作，根据这一线索，晚上 8 时许，民警在出租屋内将姚某擒获。16 日下午 5 时许，3 人被押回九江。

据了解，现年 20 岁的林某自幼喜欢计算机，经常穿梭于国内外各大黑客网站、论坛，积累了不少黑客经验，熟悉木马操作。而在杭州某大学计算机专业学习了近三年的计算机知识，更使其对网络技术非常精通。无意中，他从朋友处听说，在网上卖木马程序一个月能挣几万元。于是，他便开始注意收集国内其他黑客网站上的木马程序。2007 年 1 月底，林某从网上找了一个云南的网友帮他做了这个可以提供软件下载的"黑客吧"网站。很快，他手中掌握了 500 多种木马病毒，俨然成了"木马教主"，于是他通过网上购买身份证的形式用别人的身份证在各大商业银行开了几十个银行账户，随之就大肆贩卖各类木马病毒。林某说："并不是什么人都能从我的网站上下载木马程序，我要求他们出钱购买 VIP 资格才能正常下载，VIP 资格一年 388 元，终身制 588 元，他们的钱直接打到银行账户上就可以了。"今年 4 月份开始，"黑客吧"网站卖木马月收入突破 2 万元。面对生意的火爆，林某信心暴涨，他公然宣称要建全国最大网游木马基地，要成为"网络上让人闻风丧胆的大鳄鱼"、让人尊敬的

“木马教主”。为了更好地为“黑客吧”客户服务，林某通过分提成、“发工资”的形式请同学孔某、姚某来做“客服”，他们负责提供QQ在线“技术支持”及招揽生意。短短几个月时间，“黑客吧”旗下注册会员就达到了25 202人，付费VIP会员100余人，另有估计超过100人在该网站购买了各类木马。据林某交代，“黑客吧”网站目前卖木马非法所得已近10万元。

2）赌博罪

《刑法》第三百零三条规定：“以营利为目的，聚众赌博或者以赌博为业的，处三年以下有期徒刑、拘役或者管制，并处罚金。

开设赌场的，处三年以下有期徒刑、拘役或者管制，并处罚金；情节严重的，处三年以上十年以下有期徒刑，并处罚金。”

【案例10】

2010年2月，公安机关在工作中发现有人利用互联网在“淘××”赌博网站组织他人进行赌博，赌资数亿元，并从中牟利。公安机关立即展开侦查工作，经查发现赵某有重大作案嫌疑。2010年4月，公安机关将赵某、朴某、薛某、韩某抓获。

自2009年10月以来，赵某、朴某、薛某、韩某利用租用的“淘××”赌博网站，建立韩语版赌博网站，为韩国本土人员赌博提供条件。通过互联网开设股东账号发展总代理、代理及会员。在赌博网站开通后，赵某指使朴某、薛某、韩某以接受参赌人员投注的方式结算现金，收付赌博输赢款，维护赌博网站的正常运行来进行赌博。从2009年10月至犯罪嫌疑人到案期间，该赌博网站累计总投注额为近三亿韩元，折合人民币一百七十余万元，违法所得三千多万韩元，折合人民币十九万余元。

法院经审理认为，被告人赵某、朴某、薛某、韩某的行为均构成开设赌场罪，且情节严重，根据《刑法》第三百零三条第二款等规定，判处赵某有期徒刑四年，并处罚金二十万元人民币，其他三人有期徒刑两年，并处罚金七万元人民币。在该赌博网站参赌会员均触犯了《中华人民共和国治安管理处罚法》，构成赌博，根据《治安管理处罚法》第七十条的规定，对参赌人员分别作出行政拘留十日或十五日并处罚款的行政处罚。

3）制作、复制、出版、贩卖、传播淫秽物品牟利罪

《刑法》第三百六十三条规定：“以牟利为目的，制作、复制、出版、贩卖、传播淫秽物品的，处三年以下有期徒刑、拘役或者管制，并处罚金；情节严重的，处三年以上十年以下有期徒刑，并处罚金；情节特别严重的，处十年以上有期徒刑或者无期徒刑，并处罚金或者没收财产。为他人提供书号，出版淫秽书刊的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；明知他人用于出版淫秽书刊而提供书号的，依照前款的规定处罚。”

【案例11】

2007年1月，犯罪嫌疑人涂某化名“金先生”在网上申请了一个域名，并制作网页“黑玫瑰服务中心”，后更名为“深圳性息”。其在互联网上发布淫秽文章25篇、淫秽图片25幅、淫秽视频71个等淫秽信息供人浏览，并在网上留有招嫖信息，将其使用的手机号码公布为招嫖电话。嫖客拨打该电话与涂某联系嫖娼事宜后，涂某就打电话给张某（另案处理）安排卖

淫女到约定地点卖淫。从涂某开设网站之日直至其被抓获，共有 298 人注册为该网站会员。

法院经审理认为，涂某为了增加其网页的点击量，扩大其招嫖信息的传播范围以从中牟利，在网页上传播淫秽图片、文章和视频，其行为已构成传播淫秽物品牟利罪；涂某与莫某、雷某分别通过网上招嫖信息和派发色情卡片的方式介绍他人卖淫，其行为均已构成介绍卖淫罪，遂一审分别判处涂某、莫某、雷某一年至四年不等的有期徒刑，并各处罚金二千至一万元不等。

4）传播淫秽物品罪

《刑法》第三百六十四条规定，“传播淫秽的书刊、影片、音像、图片或者其他淫秽物品，情节严重的，处二年以下有期徒刑、拘役或者管制。组织播放淫秽的电影、录像等音像制品的，处三年以下有期徒刑、拘役或者管制，并处罚金；情节严重的，处三年以上十年以下有期徒刑，并处罚金。制作、复制淫秽的电影、录像等音像制品组织播放的，依照第二款的规定从重处罚。向不满十八周岁的未成年人传播淫秽物品的，从重处罚。”

【案例 12】

犯罪嫌疑人王某自 2008 年 9 月起利用计算机通过互联网登录淫秽色情网站丁香成人社区，注册成为会员后，为提高个人在网站中的级别，以主题帖子方式长期大量在该网站中传播淫秽电影链接、图片、小说，共计 1000 余个，迅速成为网站的管理人员。经鉴定有 63 个视频为淫秽物品。网站以会员注册方式进行牟利，其注册会员达 18 万之多，网站内设置多个版块，里面充斥大量淫秽小说、图片、电影，并且网站呈迅猛发展之势。

法院经审理认为，被告人王某非法传播淫秽物品，情节严重，侵犯了社会治安管理秩序，其行为构成了传播淫秽物品罪，根据《中华人民共和国刑法》第三百六十四条第一款等规定，判处王某有期徒刑六个月，缓刑一年。

7.3　主要信息网络违法案件及其处罚标准

信息网络违法案件主要指违反《中华人民共和国治安管理处罚法》的行政案件。根据违法行为所侵害的客体来划分，主要的信息网络违法案件有以下几种。

7.3.1　利用信息网络扰乱公共秩序的案件

1.《中华人民共和国治安管理处罚法》第二十五条

有下列行为之一的，处五日以上十日以下拘留，可以并处五百元以下罚款；情节较轻的，处五日以下拘留或者五百元以下罚款：

① 散布谣言，谎报险情、疫情、警情或者以其他方法故意扰乱公共秩序的；

② 投放虚假的爆炸性、毒害性、放射性、腐蚀性物质或者传染病病原体等危险物质扰乱公共秩序的；

③ 扬言实施放火、爆炸、投放危险物质扰乱公共秩序的。

2.《中华人民共和国治安管理处罚法》第二十七条

有下列行为之一的，处十日以上十五日以下拘留，可以并处一千元以下罚款；情节较轻的，处五日以上十日以下拘留，可以并处五百元以下罚款：

① 组织、教唆、胁迫、诱骗、煽动他人从事邪教、会道门活动或者利用邪教、会道门、迷信活动，扰乱社会秩序、损害他人身体健康的；

② 冒用宗教、气功名义进行扰乱社会秩序、损害他人身体健康活动的。

3.《中华人民共和国治安管理处罚法》第二十九条

有下列行为之一的，处五日以下拘留；情节较重的，处五日以上十日以下拘留：

① 违反国家规定，侵入计算机信息系统，造成危害的；

② 违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行的；

③ 违反国家规定，对计算机信息系统中存储、处理、传输的数据和应用程序进行删除、修改、增加的；

④ 故意制作、传播计算机病毒等破坏性程序，影响计算机信息系统正常运行的。

7.3.2 利用信息网络侵犯人身权利、财产权利的案件

1.《中华人民共和国治安管理处罚法》第四十二条

有下列行为之一的，处五日以下拘留或者五百元以下罚款；情节较重的，处五日以上十日以下拘留，可以并处五百元以下罚款：

① 写恐吓信或者以其他方法威胁他人人身安全的；

② 公然侮辱他人或者捏造事实诽谤他人的；

③ 捏造事实诬告陷害他人，企图使他人受到刑事追究或者受到治安管理处罚的；

④ 对证人及其近亲属进行威胁、侮辱、殴打或者打击报复的；

⑤ 多次发送淫秽、侮辱、恐吓或者其他信息，干扰他人正常生活的；

⑥ 偷窥、偷拍、窃听、散布他人隐私的。

2.《中华人民共和国治安管理处罚法》第四十七条

煽动民族仇恨、民族歧视，或者在出版物、计算机信息网络中刊载民族歧视、侮辱内容的，处十日以上十五日以下拘留，可以并处一千元以下罚款。

3.《中华人民共和国治安管理处罚法》第四十九条

盗窃、诈骗、哄抢、抢夺、敲诈勒索或者故意损毁公私财物的，处五日以上十日以下拘留，可以并处五百元以下罚款；情节较重的，处十日以上十五日以下拘留，可以并处一千元以下罚款。

7.3.3 利用信息网络妨害社会管理的案件

1.《中华人民共和国治安管理处罚法》第五十二条

有下列行为之一的，处十日以上十五日以下拘留，可以并处一千元以下罚款；情节较轻

的，处五日以上十日以下拘留，可以并处五百元以下罚款：

① 伪造、变造或者买卖国家机关、人民团体、企业、事业单位或者其他组织的公文、证件、证明文件、印章的；

② 买卖或者使用伪造、变造的国家机关、人民团体、企业、事业单位或者其他组织的公文、证件、证明文件的；

③ 伪造、变造、倒卖车票、船票、航空客票、文艺演出票、体育比赛入场券或者其他有价票证、凭证的；

④ 伪造、变造船舶户牌，买卖或者使用伪造、变造的船舶户牌，或者涂改船舶发动机号码的。

2.《中华人民共和国治安管理处罚法》第五十四条

有下列行为之一的，处十日以上十五日以下拘留，并处五百元以上一千元以下罚款；情节较轻的，处五日以下拘留或者五百元以下罚款：

① 违反国家规定，未经注册登记，以社会团体名义进行活动，被取缔后，仍进行活动的；

② 被依法撤销登记的社会团体，仍以社会团体名义进行活动的；

③ 未经许可，擅自经营按照国家规定需要由公安机关许可的行业的。

有前款第三项行为的，予以取缔。

取得公安机关许可的经营者，违反国家有关管理规定，情节严重的，公安机关可以吊销许可证。

3.《中华人民共和国治安管理处罚法》第五十五条

煽动、策划非法集会、游行、示威，不听劝阻的，处十日以上十五日以下拘留。

4.《中华人民共和国治安管理处罚法》第六十八条

制作、运输、复制、出售、出租淫秽的书刊、图片、影片、音像制品等淫秽物品或者利用计算机信息网络、电话以及其他通信工具传播淫秽信息的，处十日以上十五日以下拘留，可以并处三千元以下罚款；情节较轻的，处五日以下拘留或者五百元以下罚款。

5.《中华人民共和国治安管理处罚法》第六十九条

有下列行为之一的，处十日以上十五日以下拘留，并处五百元以上一千元以下罚款：

① 组织播放淫秽音像的；

② 组织或者进行淫秽表演的；

③ 参与聚众淫乱活动的。

明知他人从事前款活动，为其提供条件的，依照前款的规定处罚。

6.《中华人民共和国治安管理处罚法》第七十条

以营利为目的，为赌博提供条件的，或者参与赌博赌资较大的，处五日以下拘留或者五百元以下罚款；情节严重的，处十日以上十五日以下拘留，并处五百元以上三千元以下罚款。

习　　题

1. 信息网络违法犯罪案件的管辖范围通常是如何划分的?
2. 简述主要信息网络违法案件的种类及其处罚标准。
3. 简述主要信息网络犯罪案件的种类及其处罚标准。
4. 简要说明信息网络案件办理的工作流程。

参 考 文 献

［1］ 米佳等.公共信息网络安全教程.大连：大连理工大学出版社，2008.

［2］ 米佳等.公共信息网络安全与管理.大连：大连理工大学出版社，2006.

［3］ 陈忠文等.信息安全标准与法律法规.第二版.武汉：武汉大学出版社，2011.

［4］ 马民虎等.互联网信息内容安全管理教程.北京：中国人民公安大学出版社，2007.

［5］ 公安部公共信息网络安全监察局.公共信息网络安全监察基础训练手册.北京：群众出版社，2006.

［6］ 公安部公共信息网络安全监察局.公共信息网络安全监察业务管理指挥教程.北京：群众出版社，2006.

［7］ 宁惠军等.互联网上网服务营业场所安全管理教程.北京：中国人民公安大学出版社，2007.

［8］ 马燕曹，周湛.信息安全法规与标准.北京：机械工业出版社，2005.

［9］ 庞南等.信息安全管理教程.北京：中国人民公安大学出版社，2007.

［10］ http://www.edu.cn/20011105/3008137.shtml(中国教育与科研计算机网).

［11］ http://www.law-lib.com/law/law_view.asp? id=82529(法律图书馆).

［12］ http://www.chinalawedu.com/falvfagui/(法律教育网).

［13］ http://wenku.baidu.com(百度文库).

［14］ http://baike.baidu.com(百度百科).